Infrastrutture per il telelavoro

Prof.Ing.Linus Michaeli

Materiale di studio per la formazione a distanza
2006

Autore: Linus Michaeli ©
Revisori: Tito Livio Mongelli, Giuseppe Sabatini

Premessa

Il telelavoro è un modo efficiente per coinvolgere, nello stesso processo di produzione, lavoratori dislocati in diverse aree geografiche. Lo strumento attraverso il quale ciò è possibile è rappresentato dall'utilizzo della *Information and Communication Technology.*

Il telelavoro si ritrova quando l'*Information and Communication Technology* (ICT) viene utilizzata per consentire di lavorare a distanza rispetto al luogo in cui il lavoro viene svolto normalmente.

Prima di tutto è necessario assicurarsi che il telelavoro abbia il supporto di tutti i soggetti coinvolti. L'esperienza suggerisce che gli schemi di telelavoro vincenti sono quelli che non dipendono unicamente dall'entusiasmo del manager, ma possiedono l'appoggio di tutta l'organizzazione nel suo complesso.

E' essenziale capire le problematiche associate ad uno progetto pilota di telelavoro. La consapevolezza dei vantaggi del telelavoro sia per gli impiegati che per i datori di lavoro, aiuta a decidere come implementare il telelavoro dentro l'organizzazione.

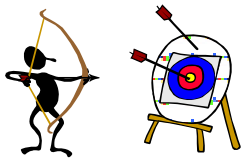
A livello strategico, affinché il telelavoro venga inserito efficientemente, è necessaria una pianificazione dettagliata.

Il telelavoro deve essere volontario e nessun impiegato deve essere costretto a parteciparvi.

L'implementazione è un processo che si realizza passo dopo passo e un piano di azione gestionale, che verrà descritto nel seguito, può aiutare a massimizzare i vantaggi potenziali del telelavoro, minimizzando problemi e rischi.

Contenuti

1. Modelli di telelavoro



Scopo

In questo capitolo verranno descritti diversi modelli di telelavoro e ne verranno evidenziati i pro e i contro.

Obiettivi

Ci si propone di:

• Descrivere i principali modelli di telelavoro;

• Offrire esempi di telelavoro per diverse aree.

1.1 Introduzione

Dal punto di vista della pratica professionale il telelavoro può essere organizzato sulla base di quattro differenti modelli:

a) Telelavoro domiciliare;

b) Telelavoro mobile;

c) Centro di telelavoro;

d) Telelavoro in una impresa virtuale.

1.1.1 Telelavoro domiciliare

E' la forma che implica la più alta dispersione dei lavoratori rispetto alla sede della società. La sua implementazione può essere vista sotto diversi aspetti: Si può considerare per esempio la formula contrattuale (lavoro dipendente, subordinato, prestazione professionale), oppure la modalità con cui si è collegati all'ufficio centrale (con o senza una connessione telematica), o ancora la tipologia della prestazione (contenuti professionali alti o bassi), l'utilizzo degli spazi (lavorare da solo a casa oppure alternare la presenza con qualcuno nello stesso posto) e del tempo a disposizione (orari e giorni di lavoro fissati oppure una gestione flessibile del tempo).

Attraverso il telelavoro a domicilio è possibile svolgere diverse attività professionali, per esempio:

- Telemarketing
- Custormer satisfaction
- Supporto tecnico (Help Desk)
- Ricerche di mercato
- Data Entry
- Organizzazione mostre e congressi
- agenzia immobiliare
- uffici finanziari
- Ricerca e selezione del personale
- Management
- Ingegneria
- Architettura
- Giornalismo
- Ricerca
- Grafica
- Design

E moltissime altre.

1.1.2 Telelavoro mobile

E' una tipologia di telelavoro che corrisponde al massimo livello di mobilità di individui coinvolti ed è anche la forma di telelavoro più diffusa al giorno d'oggi. Il telelavoratore non ha un posto fisso, ma si muove da un posto ad un altro e comunica con l'ufficio centrale attraverso strumenti portatili (ricetrasmettitori, telefoni cellulari, pc portatili che si connettono ad Internet).

La separazione dall'ufficio non è assoluta e sono contemplate anche visite sul posto e contatti periodici.

Questa tipologia di telelavoro può essere utilizzata da:

- Agenti di vendita
- venditori
- Manager
- giornalisti
- Consulenti
- Professionisti in genere

È una modalità di telelavoro molto diffusa in Europa. Le società che lo utilizzano in modo massiccio sono la IBM e la Telecom, ma ricorrono ad esso anche molte

società farmaceutiche. In Europa l'esperienza più rilevante di telelavoro mobile in termini di impiegati è quella della British Gas, dove 6500 tecnici utilizzano un portatile per tenersi in contatto con l'ufficio ed ottenere gli indirizzi dei clienti da visitare. Il telelavoratore, autonomo o dipendente, svolge la sua prestazione presso le strutture della società o presso clienti della società stessa.

1.1.3 Centro di telelavoro

Il centro di telelavoro è un luogo distante sia dall'edificio della società che da quello del cliente. È equipaggiato con dispositivi adatti alla trasmissione e ricezione dati (rete ISDN, parabola, sistemi di videoconferenze, multimedia software), che supportano l'attività lavorativa vera e propria (stazioni di lavoro, PC con programmi e software multimediali CAD/CAM) e che possono essere corredati di servizi quali mensa aziendale, servizi di navetta per i telelavoratori, etc. La struttura può essere pubblica o privata. Spesso, due o più società autonome danno vita a consorzi e istituiscono telecentri in cui lavorano i dipendenti delle diverse società con un notevole ridimensionamento dei costi di gestione. La stessa struttura privata può anche decidere di affittare delle postazioni di telelavoro ad altre società che lo richiedano. I centri di telelavoro possono essere urbani (come il centro Nexus di Telecom Roma) o rurali (come il telecentro di Castelnuovo nei Monti ed i nove telecentri che sono stati pianificati per il gruppo di montagne di Reggio Emilia). I modelli di telecentro differiscono in relazione alle specifiche necessità che ne suggeriscono la creazione, ma anche in relazione al Paese in cui viene sperimentata questa soluzione: si passa dal Telecottages svedese,inglese e irlandese, al Cybercafè spagnolo, alla Telehouse austriaca.

Per quanto riguarda i Paesi Extraeuropei, il Giappone è ricco di questi centri, mentre in America la loro presenza non è elevata (nonostante negli USA esistano dei finanziamenti per la loro realizzazione).

I centri di telelavoro possono essere adottati da:

- Società industriali e di servizi
- Municipi
- Province
- Comunità montane
- Altre istituzioni pubbliche
- Imprese private (a seconda del ramo di attività)
- Hotels
- Canali commerciali
- Aeroporti e grandi stazioni.

1.1.4 Telelavoro in una impresa virtuale

Molte società e molti gruppi di società sono organizzati con impianti, uffici e centri di produzione posizionati lontani tra loro. La scelta dei luoghi, dipartimenti e delle diverse divisioni dipende da una serie di fattori di diversa natura: vicinanza alle

materie prime e ai semilavorati o ad *outlet* dei prodotti, differenze nel costo delle apparecchiature e della manodopera, differenti tassazioni, etc.

Per esempio, si potrebbe trasferire l'attività di *back-office* dal centro città alla periferia, in quanto il costo delle stanze è più basso o perché si possono trovare più persone disposte a lavorare part-time e non lontane dal loro domicilio. Si potrebbe spostare l'impianto nei pressi dei confini nazionali in quanto il costo di manodopera è più basso, o il sistema di tassazione è più favorevole, giustificando così economicamente la delocalizzazioni produttiva.

La connessione telematica tra le varie sedi della società, e i telelavoratori mobili o a domicilio, rendono possibile la costruzione di una grande società virtuale.

Il dinamismo che caratterizza gli ambienti competitivi ha spinto molti imprenditori ad esternalizzare alcune attività. Il risultato di questa tendenza è stato un aumento nella quantità delle piccole e medie imprese nei servizi industriali e commerciali. Alcuni operatori appartenenti a queste società (per esempio televenditori, consulenti, operatori data entry, traduttori, etc.) lavorano direttamente dalla propria casa attraverso un PC, mentre altri (per esempio giornalisti, ricercatori, tecnici, etc.) lavorano in maniera mobile dal posto in cui si trovano nel momento particolare contingente.

Questa natura interattiva dei servizi produce un contatto remoto sempre maggiore tra il telelavoratore e il cliente, mentre diminuisce quello tra società e lavoratore. Probabilmente si andrà verso la diffusione di società prive di un luogo fisico o al più con una sua importanza marginale in cui è l'organizzazione aziendale che assume la massima importanza. Considerando la diffusione di questa nuova modalità con cui le società stanno organizzando la gestione del lavoro, è possibile notare come la definizione canonica del telelavoro (che considera solo le relazioni tra il dipendente e il luogo della società) fa coincidere pienamente la realtà con i fatti. Per questa ragione è appropriato definire il telelavoratore anche come qualcuno che interagisce in maniera remota con i clienti e i fornitori coadiuvato dall'utilizzo degli strumenti informatici.

Questionario di autovalutazione

Il telelavoro è molto conveniente per qualsiasi ufficio?

La gestione dei telelavoratori è basata sulla registrazione del tempo che dedicano al lavoro?

Quali sono i quattro modelli base del telelavoro?

Il telelavoro è meno flessibile rispetto ad un impiego regolare?

Il telelavoro riduce spostamenti, costi e spreco di tempo? Se sì, perché?

Esercizi, Attività

Argomenta le attività professionali adatte al telelavoro e guarda se alcune non sono state menzionate nella parte precedente.

Esercitazione obbligatoria

1. **Prepara un business plan per il Telelavoro per il settore di architettura degli interni.**

Dovrebbe contenere:

La lista degli eventuali clienti

La lista dei progetti pronti da offrire, con o senza l'arredamento e il montaggio

La descrizione del processo di approvvigionamento, l'analisi della domanda,

Proposta di immagine aziendale processi di offerta.

Budget previsionale e dettagli contrattuali, tempistica delle attività.

2. **Proponi come si potrebbe implementare un modello di Telelavoro nella tua società o nella tua posizione di lavoro**

Proporre una struttura organizzativa e il modo per gestire il lavoro nel tuo ufficio.

Valuta pro and contro dell'implementazione del Telelavoro nella tua società o nella tua posizione di lavoro.

Bibliografia

[1]. Matthies,P.: Telearbeit, Das Unternehmen der Zukunft, Markt&Technik, Verlag,Haar bei Műnchen,2001

[2]. Nilles, J.M.: Managing Telework, John Wiley&Sons, 1998

Conclusioni

Il telelavoro può essere organizzato secondo diversi modelli.

L'eventuale telelavoratore dovrebbe valutare all'inizio i seguenti aspetti:

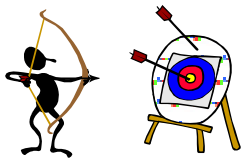
- l'adattabilità del suo lavoro al modello di telelavoro;
- requisiti tecnologici richiesti per l'attuazione del telelavoro;
- L'ambiente tecnologico rappresentato dai necessari strumenti Software e Hardware per l'implementazione sul luogo di lavoro e una rete di comunicazione accessibile;
- requisiti di legge per il telelavoro che includono la salute, la sicurezza e la pensione del telelavoratore.

2. Tecnologia IC che supporta il telelavoro.

Scopo

Il capitolo descrive gli strumenti informatici e telematici che permettono il telelavoro.

Obiettivo



Vengono fornite agli studenti informazioni su:

- Funzionalità e strumenti offerti da Internet
- Possibilità tecnologiche che permettono la connessione ad Internet
- Punti di forza e di debolezza delle modalità di connessione
- Possibilità di creazione di una rete locale in casa o nell'area ufficio.
- Strumenti necessari per la connessione ad Internet
- Possibilità di telelavoro usando altri servizi disponibili per il pubblico.

2.1 Introduzione

Il telelavoro inizia con l'email. Una volta che si conosce l'indirizzo email di qualcuno è possibile scambiarsi messaggi quando si vuole, ad un costo irrisorio, e con un alto grado di sicurezza – entrambi i destinatari possono tener traccia dei messaggi scambiati, qualora entrambi ne tengano copia. La "telecooperazione" può essere ancora aumentata grazie all'introduzione di nuove possibili attività, le principali al giorno d'oggi sono ad esempio discussioni e conferenze online, in questa maniera gruppi di più persone possono facilmente scambairsi messaggi. Per piccoli gruppi questo può avvenire usando semplicemente la copia degli indirizzi che ognuno può fare utilizzando il servizio email, mentre per gruppi più grandi si può stabilire una lista di discussione centralizzata o una più sofisticata web conference.

Le chat e i forum rappresentano un ulteriore modo di riunire persone che lavorano in luoghi geografici diversi utilizzando internet.

Tramite la condivisione delle informazioni, che oggi significa il World Wide Web, invece di mandare documenti e informazioni, ogni persona mette delle pagine su Internet che ognuno può consultare ed utilizzare. Come per le mail e i gruppi di discussione questo significa che l'informazione viene resa disponibile in qualunque parte del mondo in pochi secondi o minuti e ad un costo irrisorio per pagina.

La videoconferenza, che può utilizzare la linea Internet o una qualsiasi altra modalità di trasmissione, mette in relazione visiva le persone senza la necessità di viaggiare.

I dati dei computer e delle applicazioni condivise sul web, sono a disposizione delle persone che prendono parte all'incontro, le quali possono attivamente archiviare, manipolare e contribuire ai documenti presenti utilizzando gli strumenti delle applicazioni come per esempio fogli di calcolo, database, grafici e disegni "a distanza".

I primi quattro di questi strumenti (email, conferenze, chat e condivisione delle informazione attraverso il World Wide Web) possono essere realizzati ad un costo molto basso, prendendo in considerazioni persone che già possiedono un computer. Una videoconferenza soddisfacente e un'applicazione di condivisione richiedono una tecnologia addizionale.

I metodi che gestiscono la collaborazione del gruppo di lavoro potrebbero essere distinti in metodi di cooperazione Aperti e Chiusi.

Una telecooperazione "Aperta" si verifica quando le persone si connettono tra di loro utilizzando Internet "in pubblico" – gli utenti sono liberi di entrare o lasciare il gruppo a loro piacimento. Internet aperto supporta migliaia di aree di discussione pubblica (mailing-list, newsgroup o forum) in cui le persone si incontrano e scambiano punti di vista, condividono interessi simili e si aiutano a vicenda.

I gruppi di telecooperazione "Chiusi" possono essere reti informali di persone che sono d'accordo nel lavorare insieme e hanno adottato regole comuni, in modo tale che gli ultimi arrivati per entrare a far parte della telecooperazione devono sottostare alle regole e ai processi decisi dal gruppo, oppure possono essere inseriti molto formalmente – per esempio gli impiegati di una società, o i membri di un corpo professionale.

Al giorno d'oggi è possibile usare le funzionalità e gli strumenti offerti da Internet per telelavorare, come ad esempio:

• programmi client per la gestione delle mail, per ricevere e spedire mail e file;

• sessioni telnet per connettersi ad un terminale remoto (PC o STAZIONE DI LAVORO);

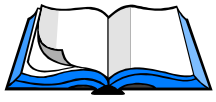
• sessioni FTP (*File Transfer Protocol*): per trasferire file ad un computer remoto, o ad un computer distante dal proprio;

• CHAT per parlare con altre persone;

• Net Meetings per gestire videoconferenze

• browser per navigare fra le pagine internet, utilizzando il protocollo HTTP (Hyper Text Transfer Protocol);

2.2 Connessione tramite una normale linea telefonica



Un computer si connette ad una linea telefonica normale utilizzando un strumento hardware chiamato modem. Il modem codifica il segnale in modo tale da essere spedito attraverso la linea telefonica standard.

Tecnologia IC che supporta il telelavoro

- Connessione ISDN
- Connessione ADSL

ISDN (Integrated Services Digital Networks) ISDN è stata la prima connessione digitale disponibile da casa e da utenti di piccole imprese. È più veloce del modem analogico, anche se non di molto infatti la linea ISDN connette a 128 Kbps, che è soltanto il doppio di una connessione a 56.6 Kbps col vecchio modem analogico. Per ottenere questo modesto incremento di velocità è necessario rapportarsi con una tecnologia costosa, instabile e poco pratica – motivo per cui, in molte aree del paese, l' ISDN è stata soppiantata dalla meno costosa (e decisamente più veloce) tecnologia DSL.

L'installazione tipica della linea ISDN richiede la visita di un tecnico della società telefonica che la gestisce. In molti casi, viene richiesta una separata linea ISDN per farla funzionare nell'abitazione; un modem ISDN (a volte chiamato borchia) viene quindi connesso a questa linea e poi al pc. L'ISDN non è sempre attiva, come invece la DSL, infatti ogni qual volta ci si vuole connettere bisogna effettuare una chiamata. (fortunatamente, effettuare una chiamata per l'ISDN è molto più veloce di una normale telefonata).

DSL (Digital Subscriber Line) DSL è una tecnologia a banda larga veloce ed in crescita, in quanto è supportata dall'esistente linea telefonica, fornisce velocità elevate e costi ridotti, questo spiega la sua crescente popolarità. (Fig. 2-1).

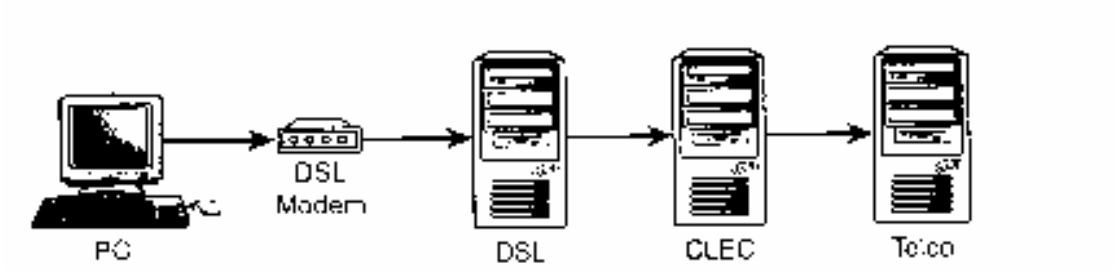


Fig.1

Fig. 2-1.Percorso da un computer che utilizza una connessione DSL

Il modem chiama l'Internet Service Provider (ISP), e si registra tramite un account personale. L'ISP ha un modem alla sua fine che traduce il segnale in ingresso in un segnale che il computer può capire.

Opzioni alta velocità – la banda larga

Anche la migliore connessione Internet può essere fastidiosamente lenta – specialmente con il crescere di siti Web che aggiungono file grafici e multimediali molto pesanti. Ogni singolo elemento che sta su un pagina Web deve essere scaricato sul computer prima di essere visto e una trasmissione a 56.6 Kbps può non essere

abbastanza veloce per scaricare tutto istantaneamente. Il risultato è che per accedere ad alcune pagine è richiesto molto tempo – e anche per scaricare file molto pesanti o ricevere mail con allegati di grandi dimensioni. Così si clicca e si attende finché l'ultimo bit trova finalmente la sua strada attraverso il modem fino allo schermo o l'hard disk, pensando ogni volta che deve esserci un modo migliore, che in realtà esiste: è la connessione a banda larga, e può velocizzare l'accesso a Internet di circa dieci volte rispetto alla corrente connessione.

2.3 Connessione banda larga tramite altre reti

Diversamente dalla vecchia linea telefonica analogica, la connessione a banda larga è un connessione digitale *end-to-end* dove tutti i dati digitali possono viaggiare più velocemente dal computer agli altri punti del Web.

Ad oggi, esistono cinque tipi diversi di connessione a banda larga digitale. Per velocizzare la connessione è possibile scegliere tra:

Linea Digitale (Fig. 2-2). I modem per la linea cablata (digitale) stanno aumentando la loro diffusione così da connettere tramite la linea digitale le singole linee che sono già presenti nelle case di tutto il Paese. Questo crea una connessione molto semplice e veloce, con una velocità minima di circa 640 Kbps ed una tipica da 2 Mbps a 4 Mbps e oltre.

Quando la DSL viaggia attraverso la linea telefonica, la banda larga occupa un determinato spazio (chiamato tunnel) all'interno del segnale che viaggia attraverso il cavo di rete della società.

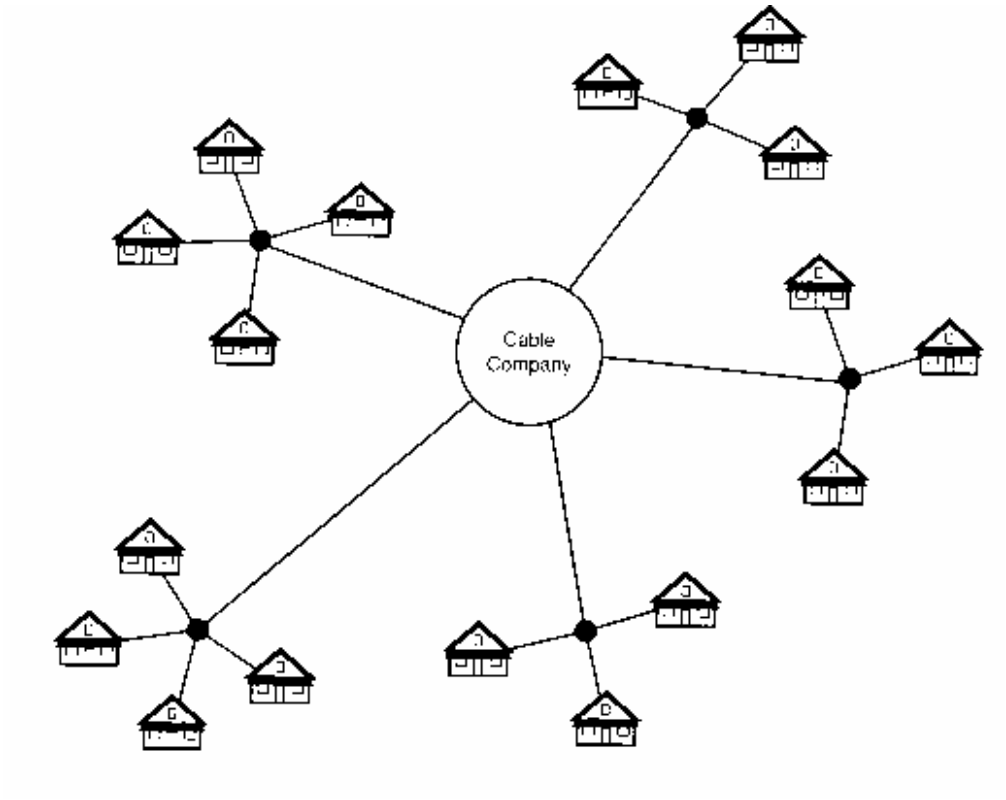


Fig. 2-2. L' accesso ad Internet via cavo si sviluppa attraverso una rete di nodi vicini – maggiore è il numero di pc connessi e minore è la velocità

Satellite (Segnale digitale via satellite) (Fig. 2-3). La stessa società che offre segnale per la TV digitale con una parabola di diametro di 18" offre anche un accesso ad internet basato sul segnale satellitare. È possibile scegliere tra un servizio *one way* (segnale veloce sul PC, lenta linea di ritorno attraverso Internet) o il servizio *two way* (segnale veloce dal satellite, e veloce anche dalla parabola allo spazio). In aggiunta, è possibile utilizzare la stessa parabola per ricevere il segnale televisivo via satellite.

Se la DSL, o banda larga non è ancora disponibile nella tua zona, c'è un ulteriore opzione: connettersi ad Internet via satellite. Ogni abitazione o impresa può ricevere segnali di dati digitali via satellite. Comunque sia, questo tipo di linea per la connessione ad internet è più lenta del collegamento via cavo o banda larga wireless, dipende da quello che ci si aspetta da una comune connessione DSL. La variazione della velocità di *upstream* (trasferimento dati in upload tramite satellite) dipende dal tipo di satellite installato.

.

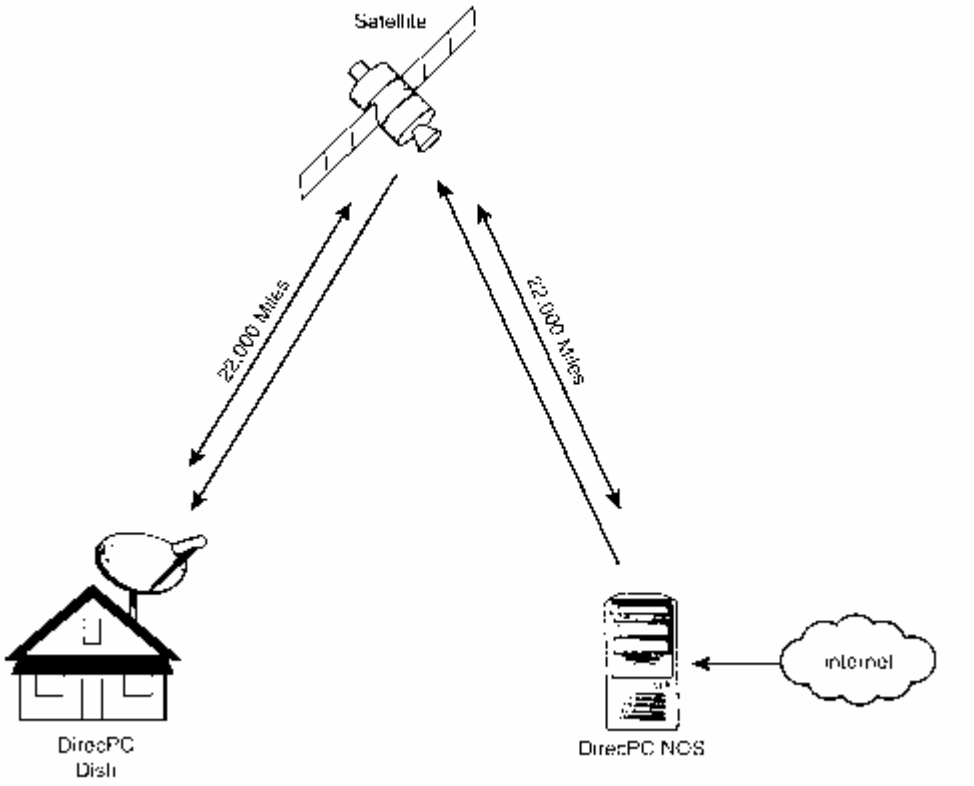


Fig. 2-1 . Connessione internet dal pc al satellite e viceversa.

Accesso banda larga senza fili (**Fig. 2-4**). Anche conosciuta come connessione *wireless*, la connessione a banda larga senza fili utilizza una tecnologia a micro-onde per trasmettere e ricevere dati Internet ad una velocità elevata.

Come la banda larga via satellite, l'accesso a banda larga senza fili permette di connettersi ad Internet senza la necessità di cavi di collegamento. Diversamente dalla banda larga via satellite (che può essere orientata quasi ovunque in Europa), la banda larga senza fili necessita di essere entro una determinata distanza dalla torre di trasmissione per evitare di perdere il segnale.

Come la maggior parte delle tecnologie a banda larga, la connessione wireless è una connessione "sempre attiva".

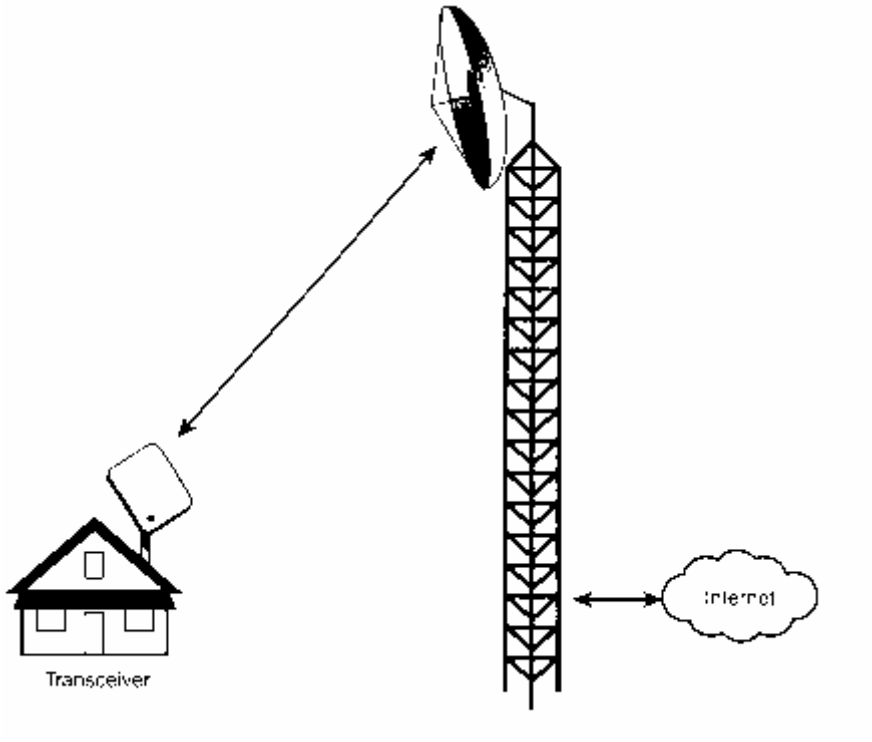


Fig. 2-2 Connessione a banda larga

2.4 Accesso a Internet per telefoni cellulari

Gli ultimi telefoni cellulari vengono costruiti con dei browser installati all'interno, e tutte le società che forniscono connessioni wireless propongono progetti che includono l'accesso al Web (Fig. 2-5).

Come funziona la connessione wireless

Come si vede dalla Fig. 2-5 le micro-onde del segnale si espandono da e verso il ripetitore. I ripetitori wireless sono disposti a distanze regolari per la massima

copertura del territorio. Molte società di cellulari offrono servizi wireless Web.

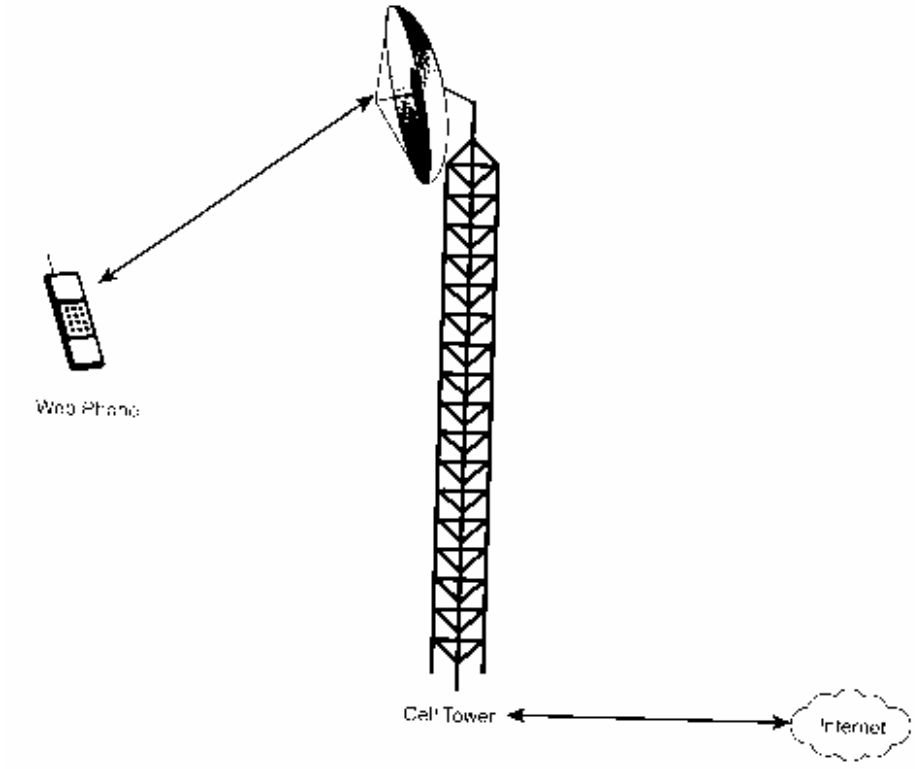


Fig. 2-5 I dati wireless Web sono trasmessi e ricevuti dallo stesso ripetitore utilizzato dai telefoni cellulari

Navigazione sul web con il WAP (*Wireless Application Protocol*)

A causa degli schermi piccoli utilizzati dai cellulari abilitati al web, la visualizzazione delle pagine web sui cellulari è diversa da come verrebbe visualizzata tramite un browser di un normale PC.

Per sormontare limitazioni relative a visualizzazioni settoriali delle pagine venne sviluppato il protocollo WAP.

Il WAP è composto da cinque protocolli separati (chiamati protocolli di stack), che lavorano tutti insieme per trasmettere e visualizzare dati web sullo schermo del cellulare dell'utente. Il protocollo per la visualizzazione, WAE, include una variante ridotta dell'HTML, chiamata Wireless Markup Language (WML), che viene utilizzata per creare pagine facilmente visualizzabili via wap. L'architettura wireless può operare in due modi:

- con connessioni *point to point* che sviluppano un'alta velocità;
- con connessioni mediante il protocollo WTP (Wireless Transport Protocol), simile al protocollo TCP/IP su Internet e che utilizza il linguaggio WML simile a HTML dal classico Internet.

I terminali possono essere telefoni cellulari, terminali dedicati, mini-browsers, news reader, client di posta elettronica.

Modem cellulari per il PC o PDA (palmari)

Un ulteriore aspetto del web wireless è aggiungere accessi ai PC fissi o ai dispositivi portatili. Si ottiene questo tipo di accesso mobile quando viene utilizzato il proprio telefono cellulare abilitato per il web come modem per il PC o il palmare o qualunque dispositivo portatile. Il telefono cellulare deve essere provvisto del servizio GPRS o UMTS (Universal Mobile Telecommunications System).

Prima che un cellulare possa essere utilizzato come un modem wireless, è necessario installare il telefono come un modem sul PC o PDA. In molti casi, questa funzione è nel software di installazione che viene dato insieme al kit di *data connectivity* del telefono (in vendita anche separatamente dal telefono). Quando viene eseguito il software di installazione il telefono cellulare è installato e configurato nel sistema operativo, e quindi è installato anche il software di gestione dei dati.

Dopo che ci si connette, i dati viaggiano dal computer fino al cellulare e poi al ripetitore più vicino, e attraverso il *gateway* del provider che fornisce il servizio escono su internet e viceversa. Al contrario della connessione WAP, nessun dato deve essere tradotto o interpretato per la visualizzazione, tutto lavora come se ci fosse un normale modem eccetto il fatto di essere senza fili (Fig.2-6).

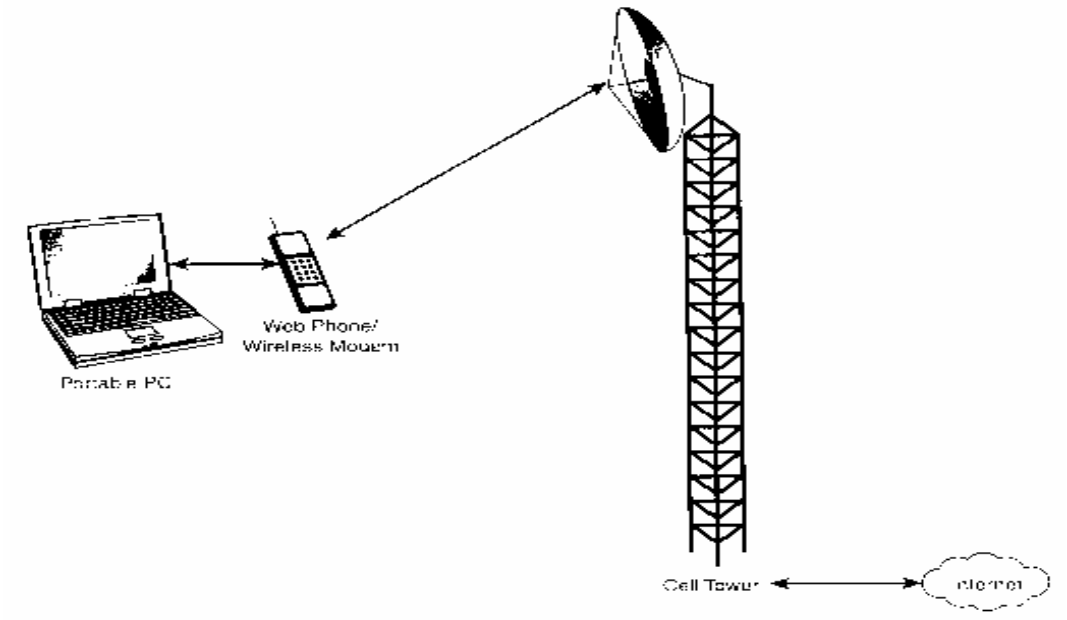


Fig. 2-6 Usare il cellulare come un modem senza fili per il portatile o il palmare

2.5 Condividere la connessione in un'area locale

Con una connessione a banda larga si ha abbastanza larghezza di banda per connettere diversi computer ad internet nello stesso momento utilizzando la stessa connessione.

2.5.1 Costruire una piccola rete

Il primo passo per condividere una connessione Internet è collegare tutti i pc con una piccola rete locale (LAN). Per fare questo bisogna installare una scheda di rete (NIC, Network interface controller) in ogni PC che si vuole introdurre nella rete. Le NIC sono delle schede che consentono lo scambio di dati all'interno della rete.

Reti senza cavi

Attualmente esistono reti per le connessioni senza l'utilizzo dei tradizionali cavi, come ad esempio la rete Wireless (WiFi) utilizza il segnale delle onde radio per collegare i computer.

Infrarossi (IrDA)

Scegliendo la configurazione. Esistono diversi modi per configurare la rete per condividere una connessione ad Internet a banda larga. La scelta dipende dalla mole di lavoro da svolgere, dalla tipologia di connessione che si vuole per ciascun PC, e dal tipo di servizio offerto dalla banda larga ISP.

2.5.2 La configurazione a ponte (bridge)

La più comune tipologia di configurazione di rete per la condivisione della connessione ad Internet è chiamata a ponte (a bridge). In questa configurazione, la connessione a banda larga gira prima sul modem, e poi sulla rete attraverso un hub o switch. Ogni PC sulla rete è connesso anche all'hub, e possiede un separato indirizzo IP statico assegnatogli dall'ISP. Una connessione a ponte è illustrata nella Fig. 2-3

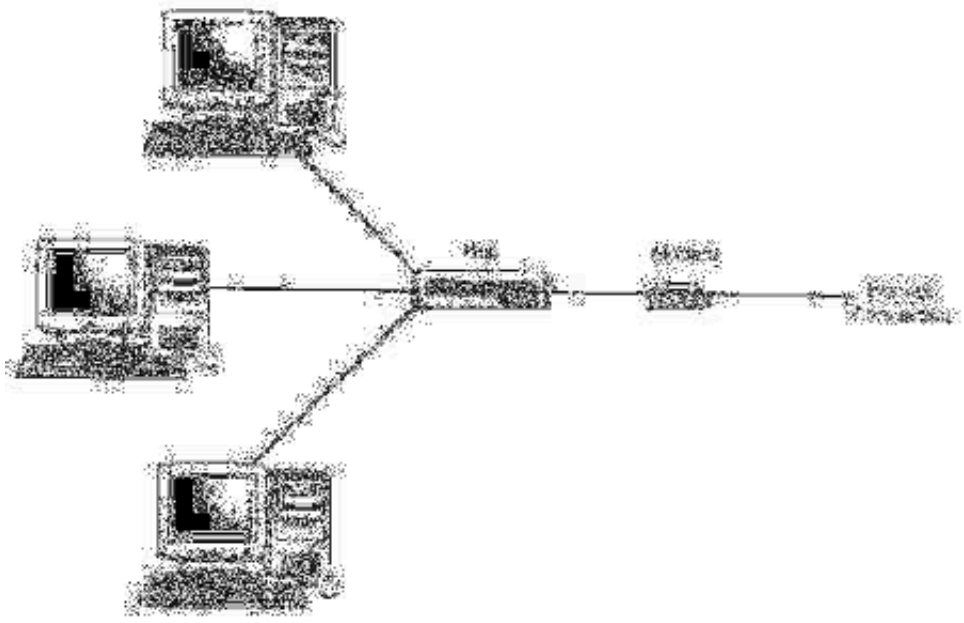


Fig. 2-3 . Configurazione a ponte per la condivisione della connessione a Internet

2.5.3 La configurazione a ponte combinata modem/ Hub

Se si è in possesso di una connessione DSL, alcuni modem hanno anche la funzione di *routing*. Per utilizzare un modem DSL come hub per connettere più PC, è necessario creare una configurazione a ponte modificata.

La configurazione gateway

Questa configurazione usa un computer server come porta ad Internet. Questo computer gateway è l'unico computer sulla rete che è visibile su Internet, e gestisce le connessioni per tutti gli altri PC. Nella configurazione gateway, il computer server funziona come una porta per l'accesso a Internet per tutti gli altri computer (Fig. 2-4).

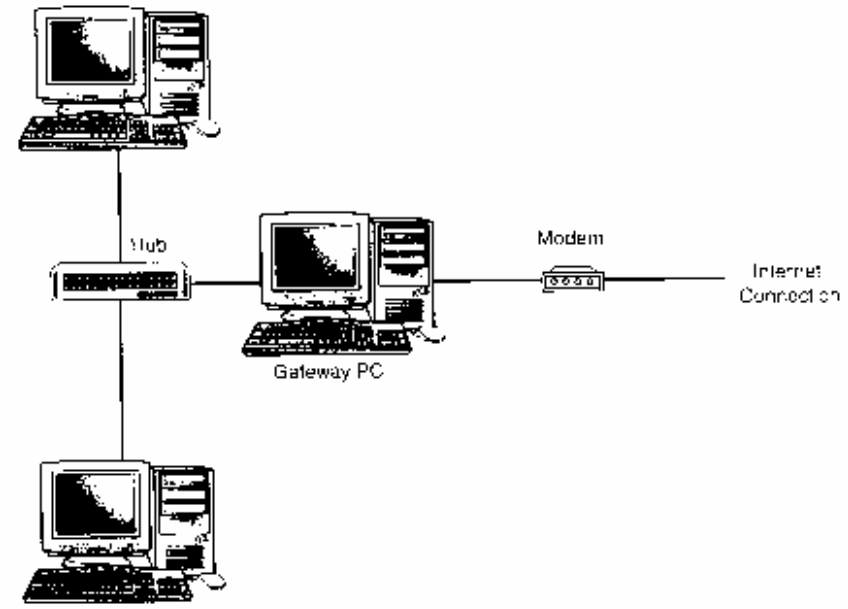


Fig. 2-4 . Configurazione Gateway. Il computer server funziona da gateway per tutti gli altri PC.

2.6 L'ISP collega il segnale tra il personal computer e Internet.

Il computer è ora connesso ad Internet, tramite l'Internet Service Provider (ISP). Dopo la connessione, è possibile accedere ad ogni sito o servizio su Internet, come ogni mail o server di news che è fornito dall'ISP. Quando il computer è disconnesso dall'ISP, non c'è connessione ad Internet, e non c'è modo di accedere a nessun sito o servizio su Internet finché non viene ristabilita la connessione.

Per connettersi ad internet è necessario possedere un account con l'Internet service provider. Quando ci si registra ad un ISP, sia l'utente che l'ISP devono fornire alcune informazioni l'uno all'altro. Il cliente fornisce solitamente il nome,

l'indirizzo, il codice fiscale, ecc, e l'ISP fornisce una serie di informazioni utili per attivare la connessione e un riepilogo dei servizi forniti dall'ISP, tra cui:

- Il numero di telefono comporre
- user name e password dell'utente
- l'indirizzo E-mail (del tipo xxx@xxx.xxx)
- i nomi dei mail server per la posta in uscita e in entrata (SMTP e POP3) che devono essere inseriti nel caso in cui si voglia settare un programma di posta elettronica
- nome and password dell'account di posta elettronica
- la lista dei newsgroup disponibili

Attività	Software
Chat	MIRC (www.mirc.com) XCHAT (www.xchat.org)
E-mail	Eudora (www.eudora.com) Microsoft Outlook Express (www.microsoft.com/windows/oe/)
FTP	FileZilla (filezilla.sourceforge.net) CuteFTP(www.cuteftp.com)
Instant Messaging	AOL Instant Messenger(www.aol.com/aim/) ICQ(www.icq.com) MSN Messenger (messenger.msn.com)
Usenet Newsgroups	Free Agent (www.forteinc.com) Microsoft Outlook Express (www.microsoft.com/windows/oe/) Netscape Messenger (home.netscape.com/computing/download/
Browser Web	Microsoft Internet Explorer (www.microsoft.com/windows/ie/) Netscape (home.netscape.com/computing/download/) Opera (www.opera.com)

Tabella 2-2 Internet e relativi software

2.6.1 Diversi tipi di ISP

Quando si considera un nuovo ISP per la connessione, c'è la possibilità di scegliere tra quattro differenti tipi di provider: ISP locali, nazionali, free e servizi commerciali on-line. Ciascuna tipologia possiede punti di forza e debolezza.

- **ISP locali.** Esistono ISP locali situati in grandi e piccole comunità in tutta l'Europa. Questi ISP sono tipicamente imprese piccole o locali che concedono l'accesso solo in ambito provinciale o regionale.
- **ISP nazionali.** Gli ISP nazionali sono grandi imprese che forniscono servizi internet a livello nazionale e possiedono punti forza e debolezza che sono diretta conseguenza dell'aumento del bacino di utenza servito.

- **ISP free.** Gli ISP gratuiti sono società che forniscono accessi dial-up gratis, in cambio della possibilità di inserire banner pubblicitari all'interno delle email inviate via web oppure all'interno delle pagine dello spazio web fornito.
- **Servizi commerciali online.** Questi servizi possiedono tutte le funzioni degli ISP nazionali, in aggiunta a una varietà di servizi e di contenuti specifici e dedicati.

2.7 Telelavoratori mobile

Se sei un telelavoratore mobile dovresti avere la possibilità di accedere alla rete globale da qualunque parte del mondo.

Quando sei fuori casa puoi accedere a tutti i tuoi account di posta elettronica, se lo avevi preventivato, e puoi fare le appropriate connessione.

Come prima cosa, è necessario procurarsi un numero di telefono locale ovunque si è (oppure nel caso sia previsto dal nostro ISP, un numero di chiamata nazionale), in modo tale da poter chiamare senza far fronte a tariffe su lunghe distanze. E se non è possibile utilizzare la normale linea telefonica o collegarsi con il proprio PC è necessario trovare un'alternativa. È possibile accedere alla consultazione della posta elettronica online (se l'ISP lo prevede fra i servizi) da qualsiasi browser.

Connessioni locali

È possibile collegarsi con il proprio numero locale, ma è un'alternativa dispendiosa visto che si pagherà una tariffa elevata per ogni minuto che si è connessi.

La soluzione migliore è ottenere un numero locale rispetto a dove si è in quel momento. Potrebbe essere problematico qualora ci si connetta normalmente ad un ISP locale che non possiede un accesso nazionale, oppure se si possiede una connessione a banda larga (come la DSL o la linea digitale) che non necessita di numeri per accedervi.

Prima di partire, dunque, è opportuno fare una lista dei numeri di accesso disponibili del nostro ISP nei vari luoghi e visionare altri fornitori per i luoghi non raggiunti dal nostro ISP (o al massimo nelle città dove si pensa si dovrà viaggiare). Ci sono diversi modi per ottenere questo tipo di accesso locale, tra cui:

- ISP nazionali. Dato che gli ISP locali non offrono spesso un accesso nazionale, gli ISP nazionali invece si. Se si viaggia molto, è bene considerare ISP nazionali quali Tiscali, MC-Link, ecc, che prevedono per le connessioni dial-up un numero nazionale.
- Wireless. Se si possiede una accesso al web wireless, è possibile utilizzare il proprio telefono cellulare come modem wireless per il PC portatile.
- Hotel con banda larga. Molti hotel high-tech offrono ai propri ospiti una connessione ad Internet ad alta velocità. In questi casi è necessario connettere il cavo di rete della al proprio portatile, e si è abilitati senza nessun numero locale da chiamare e senza l'ISP da cambiare.

Altre opzioni per connettersi

- Internet café. L'Internet café è un piacevole posto simile ad una caffetteria con le connessioni ad Internet – e, in molti casi, con computer propri disponibili ai clienti. Normalmente si paga una tariffa a minuto o ad ora e si affitta la linea bevendo un cappuccino o un tea mentre si naviga.
- Biblioteche pubbliche. Molte biblioteche pubbliche o scolastiche dotate di computer possiedono un accesso ad Internet gratis per tutti i clienti abituali. Magari bisogna attendere che si liberi la postazione e si è limitati rispetto al tempo per navigare, però offrono la connessione e spesso non costa nulla.
- Affitti. Molti grandi alberghi hanno i propri centri business affittabili per utilizzare strumentazioni e computer connessi ad internet.
- Connessione mobile su diversi dispositivi.

Anche se nella comunità europea la maggior parte delle persone si connette ad Internet utilizzando il proprio PC, non è così per il resto dei Paesi. In Giappone, per esempio più di cinque milioni di persone accedono ad internet tramite il proprio cellulare.

Questionario di autovalutazione

Quali sono gli strumenti di Internet adattabili al telelavoro?

Come si connette un normale PC ad Internet utilizzando la normale linea telefonica?

Quali sono le tre tecnologie a banda larga per connettersi ad Internet?

Come si utilizza il telefono cellulare per accedere ad Internet?

Quale è il protocollo che consente la navigazione attraverso il telefono cellulare?

Fornire i dettagli dei possibili tipi di reti locali.

Descrivere le funzioni di hub e gateway.

Quali sono le differenze tra gli Internet Service Provider ISP?

Quali tipi di comunicazioni sono disponibili per un telelavoratore mobili?

Esercizi, attività

Esamina i differenti servizi internet sul tuo computer

Download un file da un protocollo FTP

Prendi parte ad una Chat

Verifica la velocità di trasferimento dati dal tuo computer all'ISP.

Esercitazione obbligatoria

Verifica la velocità di trasferimento dei dati nella LAN della tua società

Compara la velocità in diversi punti di accesso della rete locale dalle varie postazioni di lavoro di tutti i co-lavoratori in base al proprio carico di lavoro.

Bibliografia

[1]. Matthies,P.: Telearbeit, Das Unternehmen der Zukunft, Markt&Technik, Verlag,Haar bei Műnchen,2001

[2]. Miller,M.:Using the Internet and WEB, QUE, 2002

[3]. Heslop,B.,Angell,D:The Internet Business Companion,

Growing your business in the electronic ageAddison Wesley Pub.Company,1998

Conclusioni

Il telelavoro utilizza diversi servizi dell'IC Technology, come:

• E-mail

• Discussioni o conferenze online

• Chat

• Condivisione delle informazioni utilizzando il World Wide Web (www).

• Video conferenze via Internet

• sessioni Telnet per connettersi a terminali remoti (PC o STAZIONI DI LAVORO);

• sessioni FTP per trasferire file su computer remoti

• Utilizzo del protocollo http (Hyper Text Transfer Protocol);

Le reti supportate dai servizi appena menzionati sono:

- linee telefoniche;
- Connessioni a banda larga attraverso altre reti
- Connessione tramite reti mobili e protocolli Wap

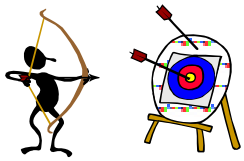
La connessione a reti locali utilizza diverse tecnologie ed incrementa la numerosità dei partecipanti tramite l'utilizzo degli hub.

3. Servizi Internet

Scopo

Il capitolo informerà gli studenti sulle procedure disponibili su Internet adattabili allo scambio di informazioni necessarie per il telelavoro.

Obiettivi



L'obiettivo del capitolo 3 è istruire gli studenti su:

- Tutti i protocolli che supportano lo scambio dei dati
- La possibilità di implementazione di videoconferenze viste come strumento complesso per una collaborazione virtuale tra i telelavoratori.
- Strumenti software per gli utenti finali che supportano il telelavoro utilizzando servizi Internet.

3.1 Introduzione

Lo sviluppo di Internet consente di diffondere i dati per il telelavoro utilizzando diversi protocolli, ognuno adatto ad ogni differente tipo di dato. L'implementazione del software aiuta i telelavoratori nella gestione del telelavoro con procedure integrate per accedere a Internet.

3.2 Protocolli Internet

L'**HTTP** è il protocollo utilizzato per la navigazione Internet, per muoversi fra le pagine web. Una società può costruire un sito web da sola, i cui contenuti sono continuamente aggiornabili, per pubblicare e quindi rendere disponibili sul web ai suoi telelavoratori documentazioni e servizi: circolari, servizi di comunicazione, data base, programmi utilizzabili da remoto, formulari interattivi, etc. Il telelavoratore (come ogni altro utente Internet) può accedere al sito della società avendo un computer, un browser di navigazione installato (il browser è un programma per la navigazione web) e digitare nel browser l'indirizzo http. Una piattaforma per il telelavoro che utilizza il protocollo http è, per esempio, il BBS (Bulletin Board System - un computer che utilizza un software per permettere a utenti esterni di connettersi ad esso attraverso la linea telefonica, dando la possibilità di utilizzare funzioni di messaggistica e file sharing centralizzato) a cui i telelavoratori possono accedere per mezzo del browser web direttamente dal loro Pc. Nel caso in cui venga installato all'interno di una rete aziendale sarà possibile accedervi senza passare per l'Internet Service Provider. Il BBS può essere organizzato sulla base di un documento **HTML** (Hyper Text Mark-up Language), come una normale pagina web visibile su Internet. In entrambi i casi è possibile condividere i documenti tra tutti gli

utenti della rete o consentire l'accesso soltanto ad alcuni utenti identificati da un indirizzo IP del computer da cui si connettono e/o dalla username e password.

Attraverso il protocollo **Telnet** è possibile accedere ad un computer remoto per controllarlo come se fosse di fronte a noi; il sistema remoto di solito richiede una username ed una password per consentire l'accesso e l'unica restrizione sta nel fatto che l'interfaccia usata non è di tipo grafico ma di tipo testuale.

Il protocollo **FTP** (File Transfer Protocol - protocollo di trasferimento file) consente gli utenti di trasferire dati in maniera affidabile ed efficiente da e verso una macchina remota. Attraverso l'FTP è possibile inviare e prendere file di ogni formato, una volta stabilita la connessione dalla parte dell'utente attraverso la username e password.

Il protocollo NNTP (Network News Transfer Protocol) è utilizzato per la gestione dei newsgroups (gruppi di discussione). Consente la creazione di una piattaforma elettronica dove ogni utente può lasciare messaggi e visionare quelli inviati dagli altri utenti. I messaggi vengono archiviati sui *news server* e sono disponibili per gli utenti via browser. Questo protocollo non ha nulla a che vedere con quelli utilizzati per lo scambio di mail come il POP3 e SMTP, che sono protocolli standard per lo scambio delle email.

E-mail e Chat sono degli strumenti molto utili per il telelavoro interattivo. Le email consentono di spedire testi con file allegati di vario tipo (grafici, immagini, etc.). L'invio e la ricezione delle mail in termini temporali richiede soltanto pochi minuti e **non è necessario essere connessi** ad Internet per visionare le e-mail, qualora siano già state salvate sul proprio computer. È possibile accedere alla propria casella di posta elettronica qualunque postazione Internet che sia provvista di un web browser.

La Chat, invece, consente il trasferimento immediato di testo; consente di comunicare, in tempo reale e ad un costo irrisorio con tanti utenti connessi a Internet **in maniera attiva**, indipendentemente dal un posto fisico dove si risiede.

3.3 La videoconferenza

Utilizzando un PC fornito di webcam, microfono e una connessione internet si può attivare una conversazione face-to-face e utilizzando i seguenti servizi di NetMeeting:

Conferenze video e audio. L'audio e video conferenza tramite NetMeeting consente ai telelavoratori di comunicare tra loro e con chiunque via Internet.

Whiteboard. Il whiteboard è una sorta di blocco per gli schizzi condiviso fra i vari telelavoratori.

Chat. La Chat permette ai telelavoratori di avere conversazioni in tempo reale utilizzando testo, con quante persone si vuole.

Trasferimento file. Il trasferimento dei file consente l'invio di uno o più file in background durante una conferenza.

Condivisione programmi. Il programma di condivisione programmi di NetMeeting consente l'utilizzo condiviso di più programmi durante una conferenza e mantiene il controllo del loro utilizzo.

Condivisione del desktop remoto. Consente a più telelavoratori di lavorare sullo stesso computer da computer remoti.

Sicurezza. NetMeeting utilizza misure di sicurezza per proteggere la privacy dei telelavoratori.

3.4 Software che supportano il telelavoro

Lo strumento software chiamato *groupware* (o software collaborativo) si riferisce alle tecnologie pensate per facilitare e rendere più efficace il lavoro cooperativo da parte di più persone. I programmi di groupware sono dedicati al lavoro di gruppo in cui si verifica uno scambio coordinato di informazioni tra i telelavoratori. Le funzioni tipiche del groupware sono:

- Gestione delle mail
- Gestione e registrazione di documenti web sviluppati in tempi differenti da diversi membri del gruppo lavorativo.
- Possibilità di organizzare riunioni del gruppo.
- Gestione di un'agenda comune dei membri del gruppo

Attualmente gli strumenti software esistenti sono: Notes, Domino e Outlook-Exchange.

3.4.1 Lotus Notes e Domino

Lotus Notes è un sistema client-server per il controllo delle applicazioni di lavoro in un gruppo. Ogni applicazione costituisce il database che contiene i documenti principali, i formulari e le relazioni. Ogni documento contiene campi, che potrebbero essere accessibili da ogni database come Titolo, Autori, Dati etc. La creazione di un documento deve essere fatta attraverso la compilazione di moduli. Lotus Notes permette la condivisione di informazioni indipendentemente da dove si trovano i componenti del gruppo usando la funzione "replica", che consente di duplicare il contenuto del database ad altri server, ovunque si trovino. L'obiettivo principale della funzione replica è sincronizzare tutti i documenti di lavoro senza l'intervento manuale di qualcuno. Le funzioni relative ai messaggi sono utili per le comunicazioni interpersonali, la gestione degli incontri online o l' organizzazione di meeting in rete.

Grazie all'integrazione con il server http, Lotus Domino e Notes consentono di scambiarsi informazioni tra il database Notes e il Web con un semplice accesso alle applicazioni esistenti sul server tramite l'utilizzo di semplici browser.

I documenti, i report e il modulo Notes potrebbero essere automaticamente convertiti in pagine HTML. Un esempio dell'utilizzo di Lotus Domino e Notes è il monitoraggio e il controllo di anomalie di un prodotto.

L'operatore riceve dal cliente l'informazione sul danneggiamento dei prodotti acquistati.

L'operatore riempie il modulo (usando Notes) e inserisce la comunicazione del cliente, la data e il tempo, il nome dell'operatore, il codice del prodotto e il codice dell'anomalia in base a tabelle predefinite.

A questo punto il problema potrebbe essere o non essere conosciuto.

Sarà automaticamente confrontato con il database di difetti esistenti sul server Domino. Da questo server potrebbe essere individuata la soluzione già attuata in un caso simile e l'operatore suggerirà al cliente i passi da seguire per correggere il problema.

Qualora invece il problema non si sia mai verificato, l'operatore registrerà il problema. Dopo di ché l'operatore affiderà il caso al personale qualificato che proverà a trovare la soluzione.

3.4.2 Outlook e Exchange

Outlook è un programma di Microsoft per le e-mail e la gestione delle informazioni personali. La principale caratteristica di Outlook è la possibilità di inviare e ricevere le mail utilizzando Internet. Se il computer è connesso ad una LAN che contiene un *mail server Exchange* è possibile utilizzare Outlook per spedire e ricevere messaggi direttamente dalla LAN.

Inoltre Outlook contiene gli strumenti per l'organizzazione, la registrazione e la partizione di messaggi elettronici. Tra le componenti di Outlook è presente un modulo per la ricezione e l'invio delle news chiamato Outlook Express. Alcuni newsgroups sono privati (i partecipanti allo stesso gruppo sono autorizzati a parteciparvi) e sono accessibili dall'impresa mentre altri sono accessibili da fuori la società.

Outlook ha a disposizione uno scadenzario per gli appuntamenti e la pianificazione dei compiti giornalieri. Con lo scadenzario di Outlook è possibile annotare incontri, usarlo come memorandum e registrare gli eventi più importanti dell'anno in corso. Se il computer è connesso al Microsoft Exchange Server, Outlook offre la funzione di "Planning dei compiti (mansioni)" per l'intero gruppo di lavoro. Questa funzione consente di pianificare gli incontri del gruppo, in quanto Outlook consente di trovare degli intervalli di tempo convenienti per tutti i partecipanti del gruppo.

Tra i moduli Outlook è quello che può configurare Microsoft Internet NetMeeting, utile per la gestione degli incontri su Internet. Permette di realizzare diversi tipi di incontri sulla base degli strumenti multimediali di ogni partecipante.

Di seguito, un esempio di utilizzo per fissare un incontro sulla valutazione dei progressi di un progetto comune

1. Scadenzario che utilizzerà la lista dei partecipanti e la durata del possibile incontro.

2. Outlook in collaborazione con Exchange esamina l'agenda dei futuri partecipanti
3. Il capo progetto sceglierà fra le finestre di tempo proposte quella che è più conveniente e genera un messaggio che prenoterà il tempo scelto per l'incontro comune di tutti i partner.
4. Dopodiché ogni partner riceverà la convocazione.

Questionario di autovalutazione

Quale è l'utilizzo dei seguenti protocolli: TCP/IP, HTTP, Telnet, FTP, NNTP, POP3, SMTP, IRC

Quale è il linguaggio di programmazione per le pagine web

Quali sono le componenti di una videoconferenza.

Descrivere le principali caratteristiche di Lotus Notes per il telelavoro.

Descrivere le principali caratteristiche di Outlook e Exchange.

Le riunioni online vengono effettuate usando il programma Net Meeting

Esercizi, attività

Apri il menu del programma disponibile per il telelavoro e verifica ogni voce

Esercitazione obbligatoria

Prepara il software disponibile per il telelavoro considerando l'attività di rivenditore mobile di libri.

Bibliografia

[1]. Miller,M.:Using the Internet and WEB, QUE, 2002

[2]. Heslop,B.,Angell,D:The Internet Business Companion,

Growing your business in the electronic ageAddison Wesley Pub.Company,1998

Conclusioni

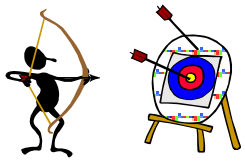
Il telelavoro via Internet utilizza diversi protocolli per ogni tipo di dato e servizio. Il software che supporta il telelavoro è adattato ai servizi Internet e alle specifiche esigenze di particolari compiti di lavoro.

4. La rete (Networking)

Scopo

Il capitolo vuole esporre le componenti dell'*Information and Communication* che consentono tutti i servizi Internet adatti al telelavoro.

Obiettivi



L'obiettivo del capitolo è far conoscere agli studenti:

• I diversi tipi di reti

• gli strumenti per la connessione dei computer attraverso le varie reti

• gli strumenti Hardware per la connessione dei computers da un'area locale alla rete.

4.1 Introduzione

Un *internetwork* è un'insieme di reti individuali, connesse tramite un dispositivo intermedio di rete, che funziona come un'unica grande rete. La parola *Internetworking* si riferisce all'industria, prodotti e procedure, che incontrano la sfida di creare e amministrare internetwork. La Fig. 4-1 illustra alcuni differenti tipi di tecnologie di rete che possono essere interconnesse da router o altri dispositivi di rete per creare un internetwork:

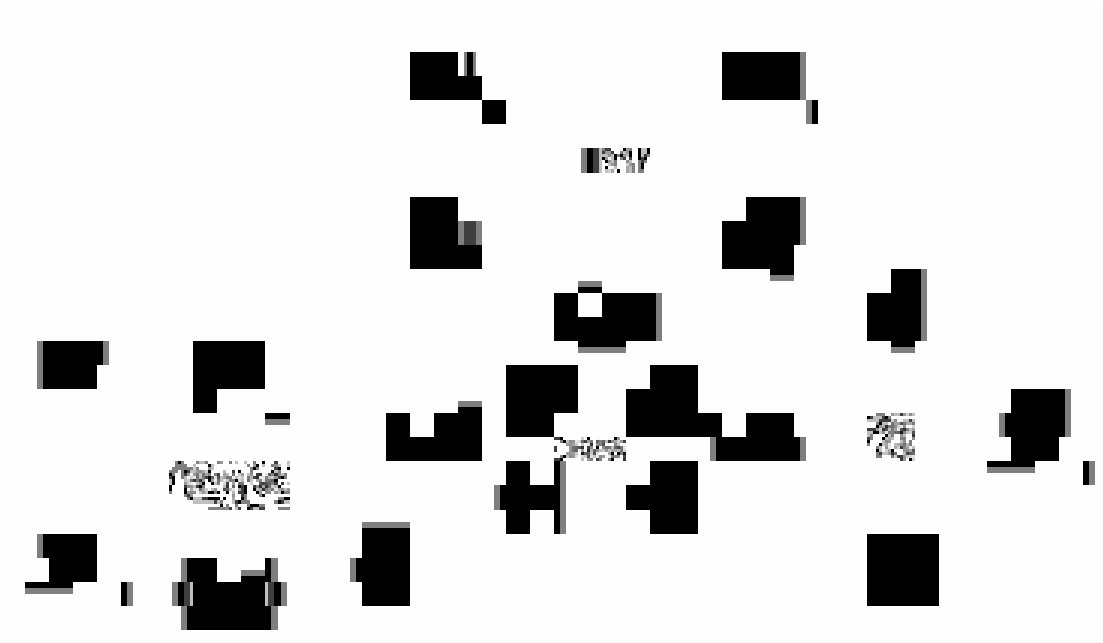


Fig. 4-1 diverse tecnologie di rete che possono essere interconnesse per creare un internetwork.

4.2 Che tipi di reti esistono?

Esistono molti tipi di reti, ma i più comuni sono la LAN (Local-Area Networks (LANs), e la WAN (Wide-Area Networks). In una LAN, i computer sono collegati all'interno di una "local area" (per esempio, un ufficio o casa). In una WAN, i computer sono distanziati e sono collegati via linee telefoniche, onde radio o altri mezzi di connessione..

Come vengono classificate le reti?

Le reti sono usualmente classificate secondo: Topologia, Protocollo, e Architettura.

La **Topologia** specifica la struttura geometrica della rete. Le più comuni sono ad anello e a stella.

Il **Protocollo** specifica un insieme di regole e segnali comuni che i computer della rete utilizzano per comunicare. La maggior parte delle reti utilizzano il protocollo *Ethernet*, ma alcune reti possono utilizzare il protocollo *Token Ring* della IBM. Il protocollo Ethernet è consigliato sia per reti domestiche che per ufficio.

L'**Architettura** si riferisce ad una delle due tipologie architetturali di rete: *Peer-to-peer* o *client/server*. In una configurazione di rete Peer-to-Peer, non c'è il server, e i computer sono semplicemente connessi tra loro in un gruppo di lavoro per condividere file, stampanti, e accesso ad Internet. Questo è più comunemente usato per configurazioni domestiche ed è consigliabile per connettere gruppi di lavoro con pochi computer. In una rete client/server, di solito è presente un computer che fa da controllore di dominio della rete (NT Domain Controller), a cui si devono loggare tutti gli altri computer. Questo server provvede a diversi servizi, incluso l'accesso ad Internet centralizzato, posta (inclusa l'email), condivisione di file, accesso alla stampante nonché garantisce la sicurezza in tutta la rete. Questo tipo di rete si trova frequentemente in configurazioni d'azienda, dove la sicurezza di rete è fondamentale.

4.3 Modello ISO/OSI (Open System Interconnection)

Quando viene richiesta una comunicazione fra computer da diversi fornitori, lo sforzo per lo sviluppo del software può essere molto difficile. Differenti fornitori utilizzano diversi formati di dati e protocolli di comunicazione che non permettono ai computer di comunicare fra di loro. Avendo riconosciuto il problema, la ISO (International Organization for Standardization) ha sviluppato un'architettura di comunicazione conosciuta come modello Open System Interconnection (OSI) che definisce gli standard per il collegamento eterogeneo fra computer.

Il modello OSI (Fig. 4-2) è formato da sette livelli. Le funzioni di comunicazione sono scomposte in ordine gerarchico. Ogni livello esegue il relativo sottoinsieme di funzioni necessarie per comunicare con un altro sistema. Ogni livello confida sul livello inferiore più vicino che svolge funzioni basilari e per nascondere i dettagli di queste funzioni. Ogni livello fornisce i servizi al livello immediatamente superiore. I livelli sono definiti in maniera tale che i cambiamenti in un livello non richiedono

cambiamenti anche negli altri. Dalla partizione delle funzioni di comunicazione in livelli, il problema è molto più gestibile.

I sette livelli del modello di riferimento OSI sono: *Application* (7), *Presentation* (6), *Session* (5), *Transport* (4), *Network* (3), *Data Link* (2), e *Physical* (1).

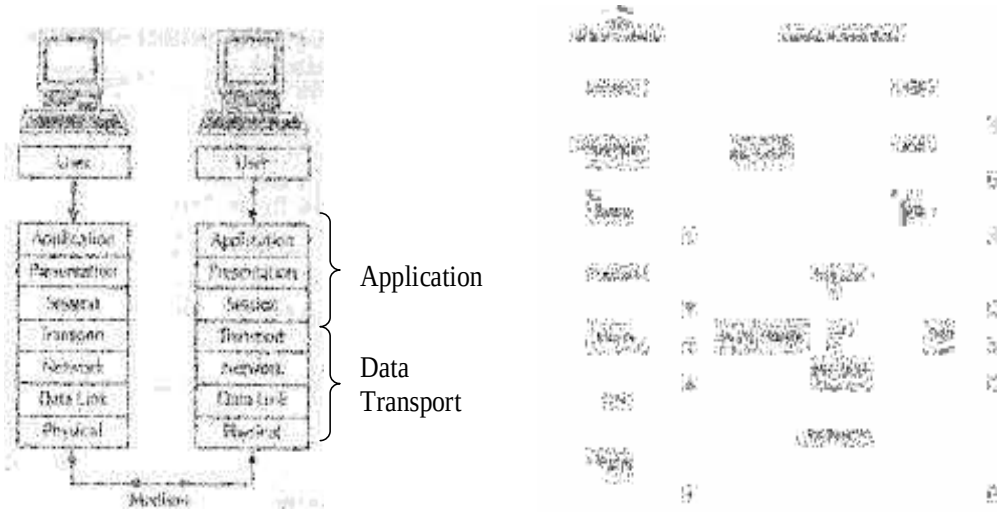


Fig. 4-2. Modello OSI e protocolli relativi con i singoli livelli

L'**Application** è il livello in cui i programmi software comunicano tra loro e stabilisce la comunicazione. I protocolli del livello Application includono WWW, FTP, Telnet, SMTP. Il livello **Presentation** controlla la conversione delle informazioni. È anche responsabile della crittografia, compressione e decompressione dei dati. Gli standard del livello Presentation includono JPEG, PICT, TIFF, MPEG, e ASCII. Il livello **Session** è responsabile della stabilizzazione e del mantenimento delle sessioni di comunicazione. Il **Transport** fornisce comunicazioni sicure. Il **Network** è il livello che fornisce il metodo per indirizzare e far passare i dati attraverso una rete. I dati sono indirizzati da un nodo ad un altro. Questo schema di indirizzamento di rete per il protocollo Internet viene trattato nel IP *Addressing*. Il **Data Link** provvede che non ci siano errori nel trasferimento di dati attraverso una rete fisica. Specifica anche la topologia della rete (come Ethernet o Token Ring). I mezzi corrispondenti sono i *bridge* e gli *switches*. Il livello **Physical** gestisce i dati nella rete e li toglie. Le specifiche del livello Physical definiscono le caratteristiche come per esempio il livello di voltaggio, di corrente, i dati fisici e i connettori fisici.

Reti:

- LAN: Local Area Network. Solitamente collegano i computer in un ufficio, un singolo palazzo o una serie di palazzi.
- MAN: Metropolitan Area Network. Reti di LAN nella città.
- WAN: Wide Area Network. Rete che ricopre vaste distanze.

Requisiti:

- Cavo: fornisce la "via" per la connessione di rete. Alcuni esempi sono la fibra ottica, coassiale, ecc.
- Scheda di rete: una scheda fissata nel computer che lo connette alla rete. I driver installati nel computer permettono la comunicazione attraverso la scheda di rete.

4.4 Hub, Bridge, Router, e Switche..

Gli hub sono blocchi che collegano molte porte ad una linea. Esistono tre categorie principali di hub: autonomi, hub accatastabili e hub modulari (Fig. 4-3).

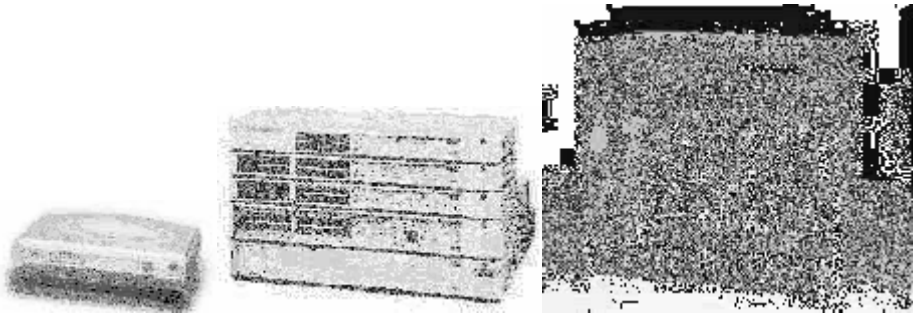


Fig. 4-3 hub autonomi (a), accatastabili (b) e modulari (c)

I bridge e i router sono strumenti utilizzati per collegare insieme LAN diverse o segmenti di una stessa LAN. I bridge sono più semplici e meno costosi dei router. I bridge prendono una semplice decisione rispetto a quali pacchetti fare/non fare passare i due segmenti che connettono. I router utilizzano le informazioni contenute in ogni pacchetto per indirizzarli all'interno della rete, e comunicano tra loro condividendo informazioni che gli consentono di determinare la migliore via nella complessa rete di tante LAN. Gli Switch sono un altro tipo di strumento utilizzato per collegare diverse LAN e dirigere i pacchetti tra di loro.

Questionario di autovalutazione

Il telelavoro richiede l'utilizzo di protocolli di trasmissione sicuri.

Quali sono le tre caratteristiche che classificano una rete?

Quanti livelli sono contenuti nel modello di comunicazione OSI?

Quali livelli sono contenuti nel modello di comunicazione OSI?

Che cosa è un hub, un router e un bridge?

Bibliografia

[1]. E.Bryan Carne:Telecommunications primer: signals,

building blocks and networks, IEEE Press 1999

Conclusioni

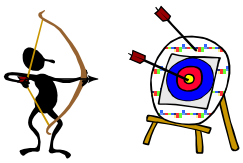
La connessione dei computer fra gli utenti in grandi aree geografiche si svolge utilizzando una rete di comunicazione globale. Questa consiste in tipi eterogenei di tecnologie ed utilizza diversi tipi di software di funzionamento. Lo scambio di dati utilizza strumenti standardizzati. La collaborazione delle diverse tecnologie si basa sulla gerarchia di standard comuni implementati in uno dei sette livelli del modello di scambio dati comune, che è chiamato il modello OSI/ISO. La connessione di più computer da una rete locale in una rete globale richiede strumenti quali hub, router e bridge.

5. Sicurezza su Internet

Scopo

Il capitolo tratta la sicurezza nel trasferimento di dati, della protezione dei dati riservati contro l'abuso e contro gli attacchi di virus per il computer.

Obiettivi



Gli obiettivi del capitolo sono:

• Descrizione degli strumenti che permettono un sicuro scambio di documenti

• Strumenti Software e hardware che proteggono il computer dai virus e da accessi non autorizzati nel pc

• Tecniche per criptare il trasferimento di dati riservati

• Strumenti per controllare persone che utilizzano speciali servizi Internet

5.1 Introduzione

La loro protezione dei dati può essere importante come proteggere altre risorse preziose, come soldi, edifici o impiegati. La soluzione per la sicurezza del computer è proteggere le sue risorse attraverso la selezione ed applicazione di appropriate protezioni.

Nel commercio elettronico, per esempio, la sicurezza è essenziale per il suo successo. La sicurezza del sistema deve esserci sia per il compratore che per il venditore su Internet in quanto potrebbero verificarsi delle frodi. Se un sistema ha utenti esterni allora i suoi realizzatori hanno la responsabilità di rendere pubblici i limiti generali delle misure di sicurezza così gli altri utenti si possono rendere conto del livello di sicurezza apportato nel sistema che stanno usando.

Ci sono tre aree di preoccupazione quando una rete accreditata è collegata ad un'altra non accreditata:

- che materiale inappropriato potrebbe deliberatamente o meno, essere trasferito da e verso la rete non accreditata;
- che utenti non autorizzati possano accedere alla rete fidata dalla rete intrusa;
- che le operazioni della rete accreditata vengano disturbate con un attacco da parte della rete intrusa.

Il computer e le misure di sicurezza di rete che vengono prese da una organizzazione sono tese a minimizzare la possibilità che si verifichino gli eventi esposti, per mezzo di quattro componenti fondamentali che costituiscono la sicurezza della rete:

1. Identificazione e Autenticazione
2. Integrità

3. Riservatezza
4. Controllo dell'accesso

5.2 Sicurezza base su Internet

I portali di e-commerce di solito sono basati su applicazioni sicure ed utilizzano il Secure Sockets Layer (SSL) per la privacy delle informazioni tra il web browser e il web server e per gli utenti utilizzino un sistema di identificazione con UserID e Password. Molte volte nei siti web viene usata meno sicurezza. E' importante capire cosa si ha con una sicurezza basilare su Internet, e ancor più importante, cosa non offre.

Dal punto di vista degli utenti, l'SSL assicura che quando si è connessi ad un sito si sta realmente comunicando con quello. SSL cripta la transazione dei dati dal proprio browser al server web. Dal punto di vista dell'impresa, o del sito web, la sicurezza in internet basata sull'SSL, la UserID e Password offre un livello rudimentale di identificazione della 'persona' che ha accesso al sito, così come autorizzazioni di base, o il controllo dell'accesso per consentire o negare l'accesso a risorse sicure di siti.

Dal punto di vista dell'utente, non si ha la segretezza dell'informazione oltre il server web, non si sa in che modo l'informazione viene immagazzinata o come si muove all'interno dell'azienda. Non si ha una forte, certificata verifica della transazione con l'impresa, la rete di fornitori o un partner. Dal punto di vista dell'impresa, la sicurezza base di internet non fornisce una buona garanzia sul trattamento dei dati, e non fornisce nemmeno la segretezza delle informazioni all'interno dell'azienda.

5.3 Maggiore sicurezza di internet

E' importante capire cosa è necessario per avere familiarità nel gestire transazioni di valore e trasportare informazioni di più alta sensibilità su internet con le nuove applicazioni disponibili. Esempi di queste nuove applicazioni includono la banche online e l'intermediazione online, gestione della cassa, il pagamento delle tasse, sistema di appalti governativo, richiesta di informazioni mediche, e il voto online. I rischi di non implementare una più alta sicurezza su internet possono variare tra la controversia o il rifiuto delle transazioni, la violazione della privacy sui dati sensibili dei clienti o dell'impresa, o l'accesso a risorse protette da individui non autorizzati. Le implicazioni di queste violazioni sono drammatiche, e variano fra la perdita finanziaria immediata e implicazioni legali a causa del non rispetto delle regolamentazioni, la perdita di fiducia degli utenti, ecc. come una breccia nella sicurezza diventata pubblica.

Il requisito fondamentale per una maggiore sicurezza su internet viene tracciato sullo spettro completo del ciclo di vita di una transazione. Questo include l'identificazione, autorizzazioni, verifica, privacy, e gestione della sicurezza.

Identificazione

E' importante capire davvero e avere la sicurezza di chi è all'altro capo della transazione o dello scambio di informazioni. Qualora non sia possibile conoscere con chi ci si sta relazionando si rischia la divulgazione delle informazioni ad individui non autorizzati. Un alto livello di identificazione può essere raggiunto utilizzando credenziali di identificazione verificate come i certificati digitali.

Autorizzazioni

Spesso c'è il bisogno di concedere o negare l'accesso a particolari risorse o applicazioni Web che si basano sull'interazione con applicazioni e/o che ruolo ricoprono. Per esempio un'organizzazione potrebbe volere diversi livelli di accesso e di risorse per i clienti, gli impiegati e i partner. Magari vorrebbero anche variare le autorizzazioni all'interno di quei gruppi. Il rischio di non implementare un sistema di autorizzazioni comporta il rischio di una maggiore diffusione di informazioni a persone non autorizzate. Senza un avanzato controllo le organizzazioni non potrebbero procedere con tante applicazioni avanzate e soluzioni di rete.

Verifica

Nell'ordine di avere una transazione che sia assicurata tra le parti, deve esserci una buona registrazione della transazione in modo tale che nessuna delle parti possa mai reclamare. Questo potrebbe essere raggiunto utilizzando firme e ricevute digitali, che ora sono anche valevoli dal punto di vista legislativo in molte giurisdizioni.

Privacy

La sensibilità delle informazioni personali o aziendali è particolarmente alta nello scambio online di transazioni e informazioni. La privacy implica tenere i dati nascosti, e mantenerli riservati durante il transito e l'archiviazione da una parte all'altra del ciclo di vita della transazione o durante lo scambio e delle informazioni. Va anche sottolineato che la privacy costituisce anche la linea di condotta per l'utilizzo e la divulgazione di queste informazioni dentro l'impresa. Il rischio di una non implementazione di un sistema di privacy sviluppato può a volte essere il problema più significativo, certamente in termini di percezione pubblica potrebbe causare una perdita di credibilità.

5.3.1 Gestione della sicurezza

La gestione della sicurezza riguarda l'abilità di gestire efficacemente ed efficientemente i requisiti appena mostrati in modo tale che ci sia meno difficoltà di amministrazione sia per gli utenti che per gli amministratori, indifferente dell'applicazione o piattaforma. Una gestione trasparente ed automatizzata della sicurezza comporta complessivamente un più basso costo di utilizzo e mantenimento del sistema.

A livello tecnologico ciò che sta all'interno della gestione di una avanzata sicurezza è l'infrastruttura **Public-Key (PKI)** o a ***chiave pubblica*.**

Il sistema che richiede una codifica con chiave pubblica e il servizio di firma digitale è conosciuto come infrastruttura *public-key* (PKI). L'obiettivo di una

infrastruttura public-key è gestire chiavi e certificati, che vengono utilizzati per l'identificazione, autorizzazioni, verifica e la privacy. Gestendo chiavi e certificati con PKI, una organizzazione è in grado di assicurare e stabilire un ambiente di rete sicuro e attendibile. Un PKI consente l'utilizzo di servizi di codifica e firma digitale nel selvaggio in moltissime applicazioni.

Attraverso la codifica, la tecnologia public-key offre riservatezza. Attraverso la firma digitale, la tecnologia comporta:

Forte autenticazione. Gli utenti possono identificarsi in modo sicuro agli altri utenti e ai server sulla rete senza l'invio di informazioni segrete (per esempio, passwords) sulla rete.

Integrità dei dati. Il controllore della firma digitale può facilmente determinare se la firma è stata modificata da quando è stata effettuata.

Supporto per il non-rifiuto L'utente che ha firmato un dato o una transazione, successivamente non può più negare di aver firmato quel determinato dato o aver partecipato ad una determinata transazione.

5.4 Sicurezza complementare

Le soluzioni per la sicurezza complementare in internet racchiudono aspetti del web, rete, e struttura dell'applicazione che non si riferiscono direttamente all'attuale transazione o scambio di dati in internet. Dove l'aumento della sicurezza di internet si serve dell'identificazione, autorizzazioni, verifica, privacy e gestione della sicurezza della transazione o dello scambio delle informazioni, la sicurezza complementare offre più consolidamento e sicurezza dell'ambiente in cui l'applicazione risiede..

Alcuni degli elementi base della sicurezza complementare di Internet includono: la rete, la sicurezza perimetro di sicurezza, la sicurezza di ingresso nella rete, soluzioni hardware di sicurezza, servizi di consulenza sulla sicurezza.

5.4.1 Sicurezza perimetrale di rete

I più comuni prodotti di sicurezza perimetrale di rete sono i firewall. Un firewall è un insieme di programmi, situati nel sever *gateway* della rete, che hanno il compito di proteggere le risorse di reti private da utenti di altre reti. Un'impresa che consente ai propri dipendenti di accedere ad internet installa un firewall per prevenire che esterni possano accedere alle risorse riservate e per controllare a quali risorse esterene accedono i propri utenti. Un firewall, lavora vicino al router, esaminando ogni pacchetto di rete per determinare se agevolarlo verso la propria destinazione. Un firewall può anche lavorare o includere un server *proxy* che fa le richieste per conto delle stazioni di lavoro degli utenti. Un firewall è spesso installato in un computer dedicato separato dal resto della rete in modo tale che non vengano effettuate richieste direttamente alle risorse di rete private, in questa configurazione tutte le richieste devono passare per il firewall.

5.4.2 Sicurezza di ingresso nella rete

Soluzioni per la scoperta di una intrusione e la valutazione di vulnerabilità sono strumenti comuni per rilevare la sicurezza di ingresso nella rete aziendale. Un sistema di ricerca di intrusioni raccoglie e analizza informazioni da varie aree all'interno della rete al fine di identificare possibili violazioni di sicurezza, che includono sia intrusioni (attacchi da organizzazioni esterne) che abusi (attacchi da dentro le organizzazioni). La scoperta di una intrusione utilizza la valutazione di vulnerabilità, o tecnologie di scansione (*scanning*) per stimare la sicurezza del sistema, del computer, o di rete.

5.4.3 Soluzioni hardware di sicurezza

La sicurezza hardware può essere utilizzata su diversi fronti inclusa l'archiviazione di informazioni private come per esempio chiavi di sicurezza, e file di operazioni di sicurezza intensiva come l'SSL (Secure Sockets Layer) o le operazioni di firma digitale. Le smart card e hardware designati sono le forme più comuni di archiviazione hardware; con questi servizi si prevengono gli attacchi alle chiavi di sicurezza. I servizi hardware svolgono anche operazioni di crittografia esclusivamente all'interno del servizio provvedendo sia ad un ambiente sicuro per accedere a chiavi segrete che per le operazioni importanti eseguite dai server.

5.5 Crittografia

La crittografia è la scienza della codifica dei messaggi, per esempio il processo di convertire un testo comprensibile e chiaro in un non comprensibile testo cifrato. Il proposito della crittografia è celare il significato del messaggio. L'obiettivo principale della crittografia è accertare che i messaggi privati non cadano nelle mani indesiderate. Negli anni sono stati sviluppati diversi sistemi crittografici al fine di provvedere alla crescente necessità di avere trasmissioni sicure di dati. I sistemi crittografici utilizzano una chiave per codificare un messaggio. La chiave è l'elemento che trasforma l'algoritmo generico di codifica in uno specifico metodo di codifica. La chiave è un sistema che genera numeri casuali di grandi dimensioni.

Sistemi crittografici

Il primo sistema crittografico utilizzato è stata la cifratura sostitutiva. Ogni lettera nel testo normale viene sostituita da un cifra, quindi il testo finale risulterà incomprensibile per coloro che non conoscono le dinamiche che regolano la sostituzione. L'efficacia della sostituzione di cifra risiede nel mantenere segreta la regola di sostituzione. Nella sostituzione in cifre, ogni lettera mantiene la sua posizione all'interno del messaggio. Nella trasposizione in cifre, invece, ogni lettera nel testo normale cambia la sua posizione nel testo cifrato, ma mantiene la sua identità.

L'evoluzione della crittografia con chiave simmetrica rappresenta una conquista nel campo della crittografia. La crittografia a chiave simmetrica utilizza la stessa

chiave per codificare e decodificare. Quindi, è necessario per entrambe le parti (mittente e ricevente del messaggio) conoscere la chiave primaria del processo di comunicazione. Utilizzando la crittografia simmetrica, è sicuro l'invio di messaggi codificati senza temere intercettazioni poiché un intercettatore non sarebbe in grado di decifrare il messaggio senza la chiave. Comunque sia, rimane sempre il difficoltoso problema di come trasferire in maniera sicura la chiave ai destinatari del messaggio, per consentirgli di decodificare il messaggio. Questa procedura diventa estremamente difficile, quando il numero delle entità aumenta (problema di gestione della chiave). C'è anche il problema di far conoscere la chiave alle persone giuste senza che il resto del mondo lo sappia (problema dello scambio di chiave).

Esistono due tipi di cifrature simmetriche (Fig. 5-1)

- Cifratura di Blocco: è un tipo di algoritmo di codifica simmetrica in cui un blocco di testo in chiaro è convertito in un blocco di testo cifrato della stessa lunghezza. La lunghezza del blocco è fissata e si chiama dimensione del blocco.
- Cifratura di Flusso: è un tipo di algoritmo di codifica simmetrica, simile alla Cifratura di Blocco, ma, mentre quest'ultima opera su grandi blocchi di dati, la Cifrature di Flusso lavora su piccole unità chiamate bit. Le cifrature di Flusso sono più veloci e molto più reperibili delle Cifrature di Blocco. Le chiavi di flusso vengono unite al testo normale usando l'operatore binario XOR per rendere il testo cifrato

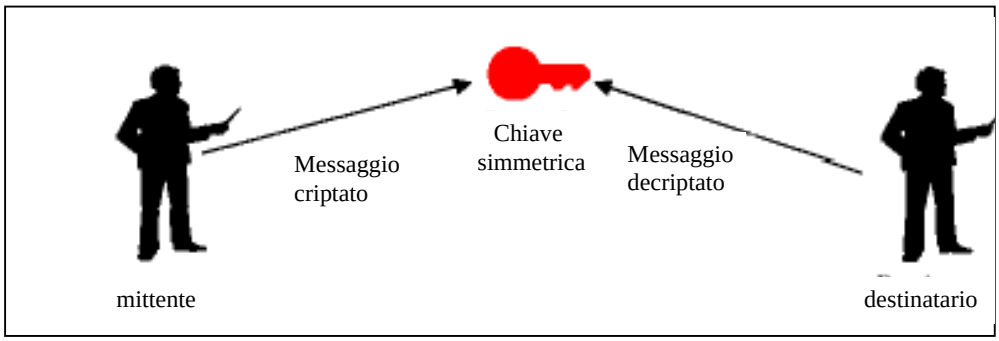


Fig. 5-1 Crittografia a chiave simmetrica

I problemi di gestione e distribuzione della chiave posti dalla crittografia a chiave simmetrica furono risolti con l'avvento della crittografia con chiave asimmetrica o pubblica. In questo tipo ogni utente ha un paio di chiavi. Il paio di chiavi è costituito da una chiave pubblica e da una chiave privata. La chiave pubblica viene generalmente usata per la codifica e la chiave privata per la decodifica del messaggio. La chiave privata dell'utente viene custodita in modo sicuro nell'hard disc, in una smart card o altri sistemi.

La chiave pubblica è inserita nel certificato digitale dell'utente (Fig. 5-2). Quando una comunicazione viene inviata, il mittente codifica il messaggio utilizzando la chiave pubblica del destinatario. Il messaggio codificato può essere decodificato esclusivamente utilizzando la chiave privata del destinatario che è conosciuta soltanto da lui.

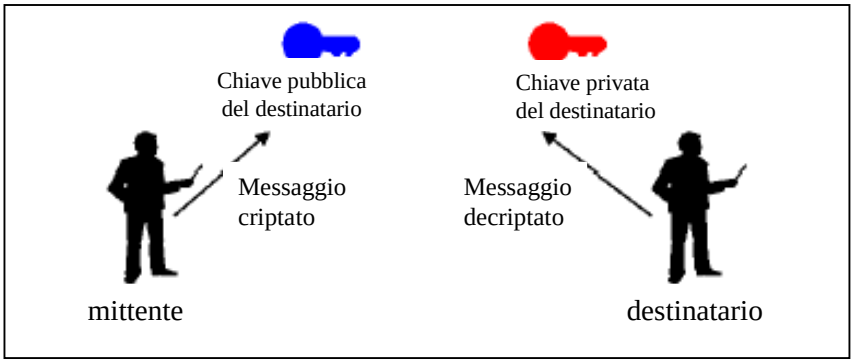


Fig. 5-2 . Crittografia a chiave pubblica

Da quando i messaggi criptati con la chiave pubblica del destinatario possono essere decriptati soltanto con la chiave privata del destinatario (che è accessibile solo dal destinatario) la segretezza dei dati trasferiti è assicurata. Le chiave pubblica è catalogata su un certificato digitale. Da quando ogni utente ha un paio unico di chiavi, il problema della gestione e distribuzione della chiave è risolto.

L'idea base della crittografia con coppia di chiavi diviene più chiara se si usa un'analogia postale, in cui il mittente è Alice ed il destinatario Bob e i lucchetti fanno le veci delle chiavi pubbliche e le chiavi recitano la parte delle chiavi private:

1) Alice chiede a Bob di spedirle il suo lucchetto, già aperto. La chiave dello stesso verrà però gelosamente conservata da Bob.

2) Alice riceve il lucchetto e, con esso, chiude il pacco e lo spedisce a Bob.

3) Bob riceve il pacco e può aprirlo con la chiave di cui è l'unico proprietario.

Se adesso Bob volesse mandare un altro pacco ad Alice, dovrebbe farlo chiudendolo con il lucchetto di Alice, che lei dovrebbe mandare a Bob e che solo lei potrebbe aprire.

Si può notare come per segretare i pacchi ci sia bisogno del lucchetto del destinatario mentre per ricevere viene usata esclusivamente la propria chiave segreta, rendendo l'intero processo di criptazione/decriptazione asimmetrico.

Firma digitale (Fig. 5-3). La firma digitale è un sistema di autenticazione di documenti digitali analogo alla firma autografa su carta.

Il sistema per la creazione e la verifica di firme digitali sfrutta le caratteristiche dei sistemi crittografici a due chiavi (sistema asincrono o a chiave pubblica). Con questo sistema la chiave pubblica di un utente è la sola in grado di poter decodificare correttamente i documenti codificati con la chiave privata di quell'utente. Se un utente vuole creare una firma per un documento, procede nel modo seguente: con l'ausilio di una funzione hash (una funzione univoca operante in un solo senso - ossia, che non può essere invertita -, utilizzata per la trasformazione di un testo di lunghezza variabile in una stringa di lunghezza fissa chiamata impronta digitale) ricava l'impronta digitale del documento, il *message digest*, un file di dimensione fissa che riassume le informazioni contenute nel documento, dopodiché utilizza la propria chiave privata per codificare quest'impronta digitale: il risultato di questa codifica è la creazione di una firma. La funzione hash, è fatta in modo da rendere minima la probabilità che da testi diversi si possa ottenere il medesimo valore dell'impronta, inoltre è *one-way*, a senso unico, questo significa che dall'impronta è pressoché impossibile ottenere nuovamente il testo originario. La firma prodotta dipende dall'impronta digitale del documento e, quindi, dal documento stesso, oltre che dalla chiave privata dell'utente. A questo punto la firma viene allegata al documento.

Chiunque può verificare l'autenticità di un documento: per farlo, decodifica la firma del documento con la chiave pubblica del mittente, ottenendo l'impronta digitale del documento, e poi confronta questa con quella che si ottiene applicando la funzione hash, pubblica, al documento; se le due impronte sono uguali, l'autenticità del documento è garantita.

Fig. 5-3 Codifica della firma digitale usando la trasformazione irreversibile Hash

Il modello ibrido di codifica (Fig. 5-4). Ogni sistema di codifica è ottimizzato per specifiche applicazioni. Un modello ibrido combina i vantaggi dei singoli sistemi crittografici in un’unica struttura. Il diagramma mostra l’adozione di una crittografia a chiave simmetrica, funzioni hash e la crittografia a chiave asimmetrica in un’unica struttura.

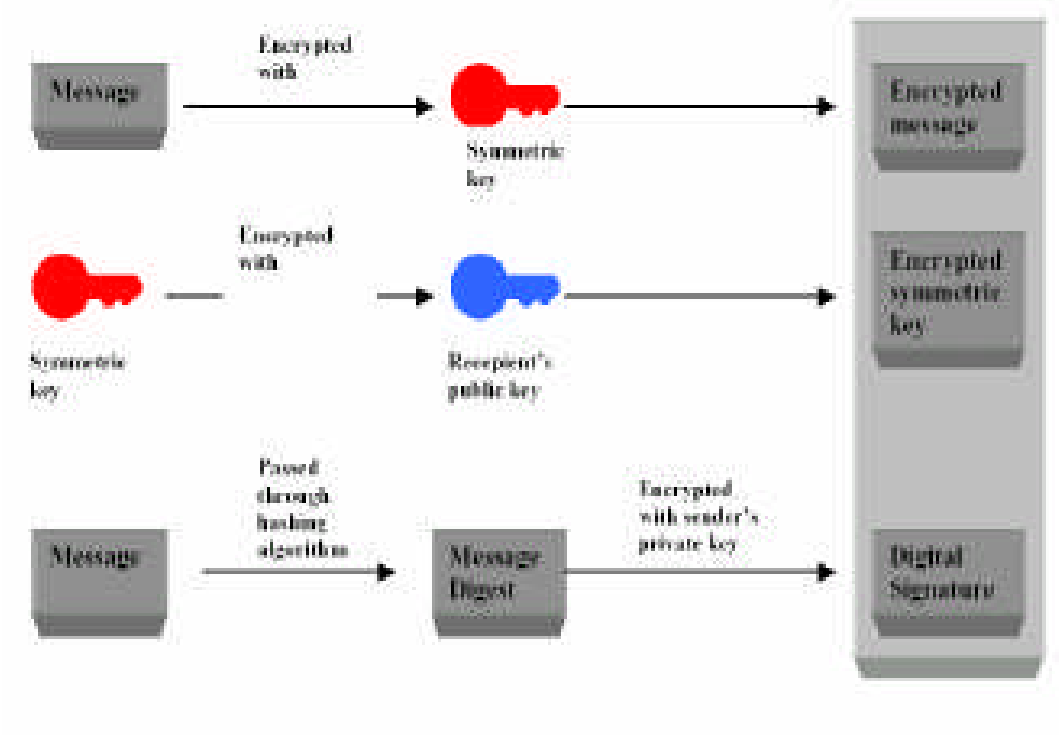


Fig. 5-4 Il modello ibrido di codifica

5.6 Protezione antivirus

Esistono diversi metodi per accedere o abusare di computer non protetti:

- login da remoto: Quando qualcuno è in grado di connettersi al computer di un altro utente e lo controlla. Questo varia dall'essere in grado di vedere o accedere ai file fino alla attivazione di programmi sul computer dell'utente.
- Applicazioni *backdoor*: Alcuni programmi possiedono delle caratteristiche speciali che consentono un accesso remoto. Altri contengono *bug* che forniscono una *backdoor* (le *backdoor* sono paragonabili a porte di servizio che consentono di superare in parte o in toto le procedure di sicurezza attivate in un sistema informatico), o un accesso riservato, che fornisce alcuni livelli di controllo del programma .
- Hijacking nella sessione SMTP: l'SMTP è uno dei metodi più comuni per inviare e–mail attraverso internet. Ottenuto l'accesso alla lista degli indirizzi e-mail, una persona può inviare robaccia indesiderata via e-mail (spam) a milioni di utenti. Questa attività viene spesso effettuata reindirizzando le e-mail attraverso il server SMTP di un insospettabile host, facendolo sembrare il mittente dello spam e rendendo il mittente reale difficile da rintracciare.
- Bug dei sistemi operativi: come le applicazioni, alcuni sistemi operativi hanno delle *backdoor*. Altri prevedono un accesso remoto con un controllo di sicurezza inferiore o possiedono dei bug da cui un hacker specializzato potrebbe trarre vantaggio.

- *E-mail bomb*: Di solito è un attacco personale. Qualcuno invia lo stesso messaggio email centinaia o migliaia di volte fino a quando il proprio sistema e-mail non riesce più ad accettare messaggi (riempimento della casella di posta)
- Macro: Al fine di semplificare complicate procedure, molte applicazioni consentono di creare uno script di comandi e collegarli ad un pulsante. Questo script è conosciuto come macro. Questa possibilità risulta vantaggiosa per gli hacker che creano le loro macro, le quali, a seconda dell'applicazione, potrebbero distruggere i dati dell'utente o mandare in crash il sistema.
- Virus: Probabilmente i virus sono i più conosciuti fra i sistemi di abuso di computer. Un virus è un piccolo programma che si copia da solo su altri computer. Così facendo può diffondersi velocemente da un sistema all'altro. I virus variano da messaggi innocui fino alla cancellazione dei dati dell'utente.
- Spam: Tipicamente innocuo ma sempre noioso, lo spam è l'equivalente elettronico di mail indesiderate. Può comunque rivelarsi nocivo. Abbastanza spesso contiene dei link a qualche sito. Bisogna prestare attenzione nel cliccare poiché si potrebbe accettare accidentalmente un cookies che prevede l'apertura una *backdoor* nel proprio computer.

5.6.1 Protezione contro i virus dei computer

Attualmente un virus per il computer è sotto molti aspetti simile ad un virus biologico: un virus biologico invade il corpo ed il suo sistema e si espande; similmente un virus per computer invade il sistema del computer e si espande anch'esso fra le varie risorse.

Un virus è un programma per computer che inietta copie di stesso all'interno degli altri programmi nel sistema del computer dell'utente. Di solito i virus invadono i programmi eseguibili e o file di sistema – il cuore del computer. Alcuni virus visualizzano solamente un messaggio noioso sullo schermo oppure inviano e-mail non richieste a tutti i contatti della rubrica; altri più disastrosi distruggono i software o le informazioni di sistema. La cosa peggiore di questo odioso gruppo è che sono sia difficili da individuare sia da eliminare in quanto si nascondono molto bene all'interno del sistema.

Come lavorano i virus

Il virus per il computer è un programma che, come già detto, piazza copie di se stesso in altri programmi del sistema, o che in qualche modo manipola altri file del sistema. La maggior parte dei virus infetta i file di programma o lavora attraverso gli script delle macro; email di solo testo non possono infettare, ma è anche vero che gli allegati delle email possono contenere virus.

Fino ad oggi sono stati scoperti milioni di virus, e possono infettare il sistema in diversi modi a seconda del tipo di virus:

- Worm. Questo tipo di virus si diffonde senza nessuna interazione dell'utente. I virus che prendono il controllo del pc e si diffondono tramite mail agli altri utenti in maniera velocissima, basta pensare a quante email si inviano e ricevono mediamente in una giornata.

- File Macro. Questo tipo di virus infetta i file, come per esempio Word o Excel. Questi virus contano sul codice di scripting contenuto negli applicativi (spesso scritti con alcune versioni di Visual Basic) per eseguire operazioni specifiche in background quando si caricano documenti nel programma applicativo.
- *Trojan Horses* (cavalli di Troia). Il Trojan è un virus nascosto all'interno di un altro programma innoquo (come uno screen sever o un'utility). Quando si avvia il programma "di copertura" si attiva il virus – similmente alla legenda del cavallo di Troia.
- File VBScript. Il VBScript è un linguaggio di scripting di proprietà Microsoft spesso utilizzato per la creazione di pagine web in HTML. Allo script è possibile collegare un virus che si attiva quando un utente visualizza la pagina che ne contiene lo script per il richiamo. Far girare uno script è come far girare un programma eseguibile; quando lo script gira, il virus è attivato.

Come prendere un virus

Ogni volta che si condividono dati con altri pc o utenti, ci si espone al rischio di potenziali virus. Agli esordi di Internet, i virus venivano diffusi dagli utenti tramite l'utilizzo e lo scambio di dischetti floppy. Il file del virus veniva salvata nel dischetto assieme al file di lavoro, e veniva copiato sul secondo PC quando l'utente accedeva ai file sul dischetto.

Oggi è più probabile che il virus venga preso da Internet. È possibile prendere un virus quando si scaricano file dal Web, o aprendo allegati di email e messaggi newsgroup sospetti.

Gli utenti, senza saperlo, infettano il loro sistema quando aprono file eseguibili allegati di un messaggio email; il messaggio è innocuo in sé, come il file allegato, fino a che non si clicca e si fa eseguire il programma. Se non si apre l'allegato, e si cancella l'email, non accade nulla. Il danno viene fatto quando vengono attivati file allegati al messaggio con estensione (fra le più frequenti) .EXE o .VBS o .COM o .BAT o .PIF.

Pratiche per la sicurezza del computer

L'unico modo per evitare la minaccia dei virus è non usare mai Internet, non condividere mai i dischetti, e non installare mai software non garantiti sul PC. È comunque possibile ridurre le probabilità di scaricarsi un virus da internet, seguendo questi suggerimenti:

- Non aprire allegati da email di cui non si conosce il mittente . Se si riceve un messaggio da un utente che non si è mai sentito prima, e il messaggio ha un allegato (un documento word o un programma eseguibile) non aprire l'allegato!! Il file word allegato potrebbe contenere un macro virus, e il programma allegato potrebbe danneggiare i dati all'intero hard disk
- Non lanciare nessun programma eseguibile allegato ad un messaggio e-mail. Questa è un'estensione del punto precedente. È buona prassi non lanciare mai nessun allegato che ha estensione del tipo: .EXE, .COM, .BAT .VBS, or .PIE
- Non eseguire programmi che si trovano sui newsgroup. I messaggi nei newsgroup spesso contengono allegati di vario tipo come programmi eseguibili.

- Non accettare file da altre persone nelle stanze delle chat. Le stanze delle chat sono un'altra grande fonte di infestazione da virus; gli utenti delle chat si scambiano file e così facendo è relativamente semplice che arrivi un virus nel passaggio, anche involontariamente.
- Scaricare programmi esclusivamente da fonti sicure. Eventualmente, usare soltanto siti web sicuri (come per esempio Download.com, Tucows, o ZDNet) i quali controllano che i file siano esenti da virus prima di consentire il download.
- Usare software antivirus. I programmi Anti-virus proteggono da tutti i tipi di virus inclusi quelli eseguibili e i macro virus. Comprare, installare e lanciare un antivirus come Norton o McAfee VirusScan e far controllare dal programma tutti i nuovi file scaricati o copiati sul sistema. Ovviamente si deve tenere il software antivirus aggiornato per proteggere il computer dai nuovi virus.

5.6.2 Prodotti antivirus sul mercato

I programmi anti-virus sono in grado di cercare virus che si conoscono e di proteggere il sistema da quelli nuovi non conosciuti. Questi programmi di default controllano il sistema ad ogni avvio e possono essere configurati in modo tale che controllino ogni programma che si prende da internet. (Per esser sicuri, sarebbe il caso si scaricare in una directory a parte i file che si prendono da internet e farli controllare dal programma antivirus prima di attivarli)

È possibile trovare vari programmi antivirus sul mercato, oppure è possibile scaricarli dalle case madri. I programmi più diffusi sono disponibili anche come servizi web, in modo tale da rendere possibile il controllo dei file online, mentre si lavora. Gli anti-virus maggiormente conosciuti sono:

- Dr. Solomon's Anti-Virus (www.drsolomon.com)
- McAfee VirusScan (www.mcafee.com)
- NortonAntiVirus (www.symantec.com/securitycheck/)
- PC-cillan (www.antivirus.com/pc-cillin/)
- Sophos Anti-Virus (www.sophos.com)

Qualunque sia l'antivirus scelto, è necessario collegarsi e scaricarsi gli aggiornamenti periodicamente in modo tale da conoscere anche i virus più nuovi, dato che nuovi virus vengono creati ogni settimana, bisogna aggiornare la lista di quelli conosciuti dall'antivirus.

5.7 Firewall

Un *firewall* fornisce un filtro che i pacchetti in entrata e in uscita devono attraversare. Il più semplice firewall dovrebbe essere un bridge Ethernet che è possibile disattivare, solo per poterlo azionare quando ci si connette ed è necessario e potrebbe essere utilizzato per tenere lontani intrusi dalla rete. La maggior parte dei firewall offre molti più servizi oltre a filtrare i pacchetti in base ai criteri settati. Un

firewall potrebbe essere una parte di un sistema operativo autonomo realizzato con l'obiettivo principale della sicurezza in internet. Ci sono anche firewall specifici che offrono solo protezione per certi tipi di servizi Internet, come i protocolli SMTP o http (posta elettronica e web).

I Firewall vengono utilizzati per due motivi:

1. Per tenere fuori le persone (virus/hacker) .
2. Per tenere le persone dentro (impiegati/bambini).

I firewall possono anche registrare l'attività di rete nel dettaglio, filtrare la registrazione per creare dei report e avvisare l'amministratore di rete quando la rete ha raggiunto una predefinita soglia o semplicemente aggiornarlo sullo spostamento dati all'interno di una rete aziendale.

Il firewall sviluppa la sicurezza di rete e riduce i rischi ai server nella rete filtrando servizi insicuri. Come risultato, l'ambiente di rete viene esposto a pochi rischi perchè soltanto selezionati protocolli possono oltrepassare il firewall.

Il problema con i firewall, è che limitano l'accesso da e a internet. Il concetto base è consentire a utenti locali di utilizzare tutti i servizi di rete all'interno della rete locale e alcuni utili servizi disponibili su internet, e controllare gli accessi degli utenti esterni alle risorse locali di rete. Esistono due tipi di firewall:

1. **Filtrazione di Pacchetto (Fig. 5-5)**. È il tipo di firewall integrato nel kernel (nucleo centrale dei comandi del sistema operativo) Linux. I firewall che filtrano i pacchetti possono essere pensati come un tipo di router. Proprio per questo è necessario avere una conoscenza approfondita della struttura dei pacchetti IP per lavorarci. Visto che vengono analizzati e registrati pochi dati, i firewall filtranti occupano meno CPU e creano meno latenza nella rete. Questi firewall non fornisco il controllo delle password e sono nascosti agli utenti che possono usare internet senza programmare le regole per il firewall.

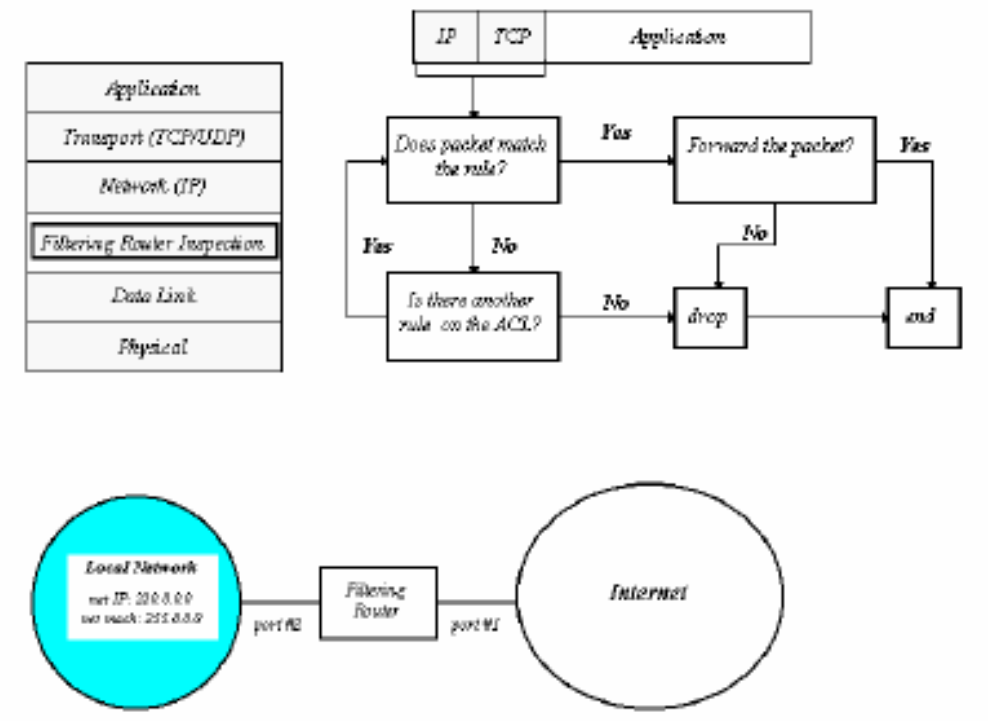


Fig. 5-5 . Firewall a filtrazione di pacchetto

2. **Server Proxy (Fig. 5-6**) sono ampliamente utilizzati per il controllo, o il monitoraggio del traffico uscente. Alcuni server proxy memorizzano i dati richiesti dagli utenti all'interno della rete, come ad esempio le pagine web: un utente dall'interno della rete si connette ad un sito esterno per scaricare alcune pagine web e il proxy ne memorizza una copia per il prossimo utente che farà richiesta delle stesse pagine che verranno stavolta scaricate dal proxy e non da internet, evitando così un sovraccarico di banda. Il server proxy offre anche la possibilità di visualizzare ciò che è stato trasferito.

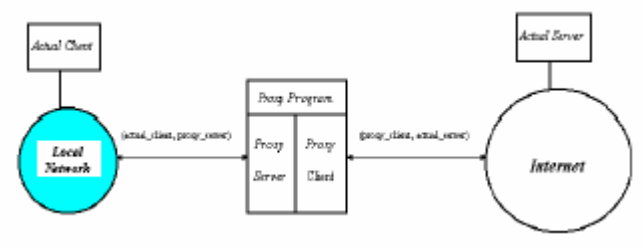


Fig. 5-6 Firewall costruito su un server Proxy

L'idea che sta alla base della componente proxy di un è non consentire una connessione diretta tra il software client sulla rete locale e il sofware server su Internet o viceversa (il software client su Internet e il software server sulla rete locale).

Invece la connessione diretta è interrotta in due separate connessioni. Il programma proxy funge da intermediario.

Mantenere il firewall funzionante

Regolare un firewall è come portare la macchina a far regolare il motore. È necessario aggiornare il firewall altrimenti potrebbe non funzionare correttamente, è bene ottimizzare operazioni e servizi, altrimenti alcuni dei componenti del firewall potrebbero non interagire al meglio fra loro.

Questionario di autovalutazione

Cosa sono i virus?

Che cos'è la codifica a chiave pubblica?

Quante chiavi utilizza il sistema di codifica asimmetrico?

A cosa si dedica il firewall?

Il trasferimento dei dati che utilizza il protocollo SSL è protetto dall'accesso non autorizzato?

Che cos'è la firma digitale e come viene protetta dall'abuso non autorizzato?

Esercizi, Attività

Controlla il tuo computer con il programma antivirus scelto, fagli fare una scansione dei virus

Esercitazione obbligatoria

Installa sul computer un programma firewall ed osserva gli eventuali attacchi dalla rete.

Bibliografia

[1]. Hance,O.:Business and Law on the Internet, McGraw Hill 1996

[2]. Miller,M.:Using the Internet and WEB, QUE, 2002

Conclusioni

Il capitolo descrive gli strumenti software e hardware per la protezione contro l'accesso dei virus e di malintenzionati ai dati protetti o sensibili. Sono stati affrontati diversi tipi di codifica con chiave pubblica, simmetrica o ibrida.